

Nasıl Yapmalı Kitapçığı

Bu Nasıl Yapmalı Kitapçığı, kendi dijital güvenliğinizi güvence altına almak için anlamanız gereken sorunları açıklamak üzere tasarlanmıştır. Bu kitapçık, karşı karşıya olduğunuz riskleri tanımlamaya ve betimlemeye ve bu riskleri en iyi şekilde azaltmak için bilgiye dayalı kararlar vermenize yardım etmenin yollarını aramaktadır. Bu amaçla temel güvenlik, verilerin korunması ve iletişim mahremiyetiyle ilgili sekiz genel soruya yanıt verir.

Her bölümün başında, belirli konuları örneklerle açıklamak ve genel sorulara yanıt vermek için bölüm boyunca kısa diyaloglarla yeniden ortaya çıkacak olan kurgusal karakterlerin rol aldığı bir arka plan senaryosu bulacaksınız. Ayrıca okuduğunuz bölümden öğrenilebilecek belirli derslerin kısa bir listesini de bulacaksınız. Okumaya başlamadan önce bu listeyi taramak iyi bir fikirdir. Bir bölüm üzerinde çalışırken, kitabın sonundaki sözlükteki tanımlara link veren bir dizi teknik terimle karşılaşacaksınız. Ayrıca araç kutusunun Uygulama Rehberi'nde tartışılan kimi yazılımlara referanslar da bulacaksınız.

Herhangi bir bölüm ya da bu araç kutusundaki herhangi bir rehber tek başına okunabilir; internet tarayıcınızdan kolay çıktı alabileceğiniz ya da elektronik olarak paylaşabileceğiniz şekilde biçimlendirilmiştir. Ancak hem kitapçığın hem de yazılım rehberinin her noktasına dağılmış ilgili bağlantıları ve referansları takip edebilirsiniz Security in-a-box'tan daha iyi faydalanabilirsiniz. Bu kitapçığın basılı bir kopyasına sahipseniz, Uygulama Rehberi üzerinde çalışırken kitapçığı önünüzde bulundurmalısınız. Nasıl Yapmalı Kitapçığı'nın belirli bir araç üzerine olan bölümünü, kendi dijital güvenliğinizi korumak için o araca itimat etmeden önce okumanız gerektiğini de aklınızda bulundurmalısınız.

Nasıl Yapmalı Kitapçığı'nın bölümlerini mümkünse sırasıyla okumalısınız. Güvenlik bir süreçtir, örneğin, bilgisayarınızı virüslerden ve diğer kötü amaçlı yazılımlardan arındırmadan, iletişim mahremiyetinizi gelişmiş bir tehdide karşı korumaya çalışmak çoğu kez yetersiz bir çabadır. Birçok vakada bu, hırsız zaten evin içindeyken kapıyı kilitlemeye benzer. Burada verilen sekiz konudan herhangi biri diğerlerinden daha önemli değildir; sonraki bölümler, şimdiye kadar bildikleriniz ve yazılım yüklemek üzere olduğunuz bilgisayarın durumu üzerine belirli varsayımlarda bulunur.

Elbette bu bölümlerin üzerinde farklı bir sırayla çalışmak istemeniz için birçok iyi neden vardır. İlk Uygulama Rehberi'nde betimlenen araçları kurmaya başlamadan önce, önemli dosyalarınızı nasıl yedekleyeceğiniz konusunda tavsiyeye gereksiniminiz olabilir. 4. Bölüm'de ele alınan Bilgisayarınızdaki hassas dosyaları nasıl korursunuz konusunu olabildiğince hızlı bir biçimde öğrenmenizi gerektiren, acil bir mahremiyet sorunuyla kendinizi karşı karşıya bulabilirsiniz. Ya da belki de güvenliği sizin sorumluluğunuzda olmayan ve herhangi bir hassas bilgiye erişmeye niyetli olmadığınız bir bilgisayarla bir internet kafede çalışıyorsunuzdur. Bu bilgisayar ülkenizde erişimi engellenmiş bir internet sitesini ziyaret etmek için kullanmak istiyorsanız, doğrudan *İnternette nasıl anonim kalınır* ve *internet sansürü nasıl aşıılır* başlıklı 8. Bölüm'e atlamanızı engelleyen hiçbir şey yoktur.

1. Bilgisayarınızı kötü amaçlı yazılımlara ve hacker'lara karşı nasıl korursunuz

Genel amaçlarınız ne olursa olsun, bilgisayarınızın sağlığını korumak, daha iyi bir güvenliğe giden yoldaki can alıcı önemdeki ilk adımdır. Bu nedenle güçlü şifreler, iletişim mahremiyeti ve güvenli silme hakkında çok fazla endişelenmeye başlamadan önce, örneğin, bilgisayarınızın *hacker* [1]lara karşı korumasız olup olmadığından ya da virüsler ve casus yazılımlar gibi, sık sık *malware* [2] olarak anılan kötü amaçlı yazılımlar tarafından istila edilip edilmediğinden emin olmalısınız. Aksi halde alacağınız diğer herhangi bir güvenlik önleminin etkililiğini güvence altına almak imkânsızdır. Her şey bir yana hırsız zaten alt kattaysa kapıyı kilitlemenin bir anlamı yoktur ve kapıyı ardına dek açık bırakarak alt katta hırsız olup olmadığını kontrol etmek de pek işinize yaramaz.

Sonuç olarak bu bölüm, yazılımınızı nasıl güncel tutmanız gerektiğini ve bilgisayarınızı her daim var olan *kötü amaçlı yazılım* [2] bulaşmalarına ve *hacker* [1] saldırılarına karşı korumak için *Avast* [3], *Spybot* [4] ve *Comodo Firewall* [5] gibi araçların nasıl kullanılacağını açıklar. Her ne kadar bu bölümde tavsiye edilen araçlar, bu tür tehditlere karşı en açık işletim sistemi olan Windows içinse de, *GNU/Linux* [6] ve Apple OS X kullanıcıları için de aynı riskler geçerlidir ve aşağıda sunulan taktikleri bu kullanıcıların da benimsemeleri gerekir.

Arka plan senaryosu

Assani Fransızca konuşulan bir Afrika ülkesinden bir insan hakları aktivistidir. Onun iki ergen çocuğu, Salima ve Muhindo, Assani'den yapması istenilen rutin bilgisayar işlerinde ona yardım etmeyi önermişti. Onlar Assani'nin bilgisayarının durumunu gördükten sonra, bilgisayarını nasıl sağlıklı ve işlevsel tutacağını temellerini öğretmeyi ona önerdi. Assani de Ücretsiz ve Açık Kaynak Kodlu Yazılımları kullanma fikrini sevdi ama bunun az ya da çok güvenli olup olmayacağı konusunda emin değildir, bu nedenle onların tavsiyesini sorar.

Bu bölümden ne öğrenebilirsiniz

- *Kötü amaçlı yazılımların* [2] bilgilerinizin mahremiyetine ve bütünlüğüne, bilgisayarınızın istikrarına ve diğer güvenlik

- araçlarının güvenilirliğine yönelik olarak ortaya koydukları birkaç belirli tehdidin doğası hakkında daha fazla şey,
- Bu tehditlere karşı kendinizi korumaya yardım etmek için tavsiye edilen bir dizi aracı nasıl kullanabileceğiniz,
 - Yazılımlarınızı sık sık güncelleyerek bilgisayarınızı nasıl güvenli kılacağınız,
 - Süresi dolan lisanslar, korsan yazılımlar ve popüler [FOSS](#) [7] araçlarına eşlik eden tehlikelerden kaçınmak ve mümkün olduğunca güvenliğinizi arttırmak için neden [ücretsiz yazılım](#) [8] araçlarını kullanmanız gerektiğini.

Virüsler

Virüsleri sınıflandırmak için birçok farklı yol vardır ve bu yöntemlerin her biri renklerle adlandırılmış kategoriler kümesiyle birlikte verilmiştir. Solucanlar, makro virüsler, truva atları ve arka kapılar bunların iyi bilinen örneklerinden bazılarıdır. Bu virüslerin birçoğu, e-postaları, kötü amaçlı web sayfalarını ya da diğer araçları kullanarak korumasız bilgisayarlara bulaşmak için internet üzerinden yayılır. Diğerleri, kullanıcının bilgi yazmasına olduğu kadar okumasına da izin veren, taşınabilir aygıtlar, özellikle USB bellekler ve harici sürücüler aracılığıyla yayılır. Virüsler, harici sürücüler üzerindeki veriler de dahil olmak üzere, bilgisayarınızdaki bilgileri yok edebilir, onlara zarar verebilir ya da onlara bulaşabilir. Bu virüsler ayrıca bilgisayarınızın denetimini ele geçirebilir ve bilgisayarınızı diğer bilgisayarlara saldırmak için kullanabilir. Neyse ki kendinizi ve dijital bilgi alışverişinde bulunduğunuz kişileri korumak için kullanabileceğiniz birçok anti-virüs aracı vardır.

Anti-virüs yazılımları

Kullanımı kolay, düzenli olarak güncellenen ve anti-virüs uzmanları tarafından saygı gösterilen [Avast](#) [3] adında Windows için mükemmel bir [ücretsiz yazılım](#) [8] anti-virüs programı bulunmaktadır. Her 14 ayda bir kaydolmanızı gerektirmektedir ancak kayıt, güncellemeler ve programın kendisi ücretsizdir.

Uygulama: [Avast! - Anti-Virüs Rehberi](#) [9] ile uygulamaya başlayın

Avast'a alternatif olarak diğer çeşitli, iyi bilinen, ticarî anti-virüs programları da vardır. [Clam Win](#) [10], [Avast](#) [3]'ün bir [FOSS](#) [7] alternatiftir. Her ne kadar birinci düzey anti-virüs programları için önemli olan belirli özelliklerden yoksun olsa da [Clam Win](#) [10]'ün avantajı, bu yazılımı kurmanıza izin vermeyen bir bilgisayarı taramak için USB bellekten çalışabilmesidir.

Anti-virüs yazılımlarını etkili bir biçimde kullanmak için ipuçları

- İki anti-virüs programını aynı zamanda çalıştırmayın. Çünkü bu, bilgisayarınızı aşırı ölçüde yavaşlatabilir ya da bilgisayarınızın çökmesine neden olabilir. Yeni bir anti-virüs programı kurmadan önce hâlihazırda bilgisayarınızda kurulu olan anti-virüs programının kurulumunu kaldırın.
- Anti-virüs programınızın güncellemeleri alabilmenize izin verdiğinden emin olun. Yeni bilgisayarlarda ön kurulumlu olarak gelen birçok ticarî aracın bir noktadan sonra kaydedilmesi (ve ücretinin ödenmesi) gerekmektedir, aksi halde güncellemeleri almaya son verir. Burada tavsiye edilen yazılımların tamamı ücretsiz güncellemeleri desteklemektedir.
- Anti-virüs programınızın kendisini düzenli olarak güncellediğinden emin olun. Her gün yeni virüsler yazılmakta ve dağıtılmaktadır. Yeni virüs tanımlarını güncellemezseniz bilgisayarınız hızla saldırılara açık hale gelebilir. [Avast](#) [3] internete bağlı olduğunuzda otomatik olarak güncellemelere bakacaktır. -Anti-virüs yazılımınızın eğer varsa virüs tarama özelliğini 'daima açık' tutunuz. Farklı araçlarda bu özellik farklı isimler altında bulunabilir ama birçok araç bunun gibi bir özellik sunmaktadır. Bu özellikler 'Gerçek Zamanlı Koruma' (Realtime Protection), 'Hane Koruması' (Resident Protection), ya da benzer bir şekilde adlandırılmış olabilir. Aracın 'Hane Tarayıcısı' (Resident Scanner) hakkında daha fazla bilgi almak için [Avast Rehberi](#) [9] 'nin [Bölüm 3.2.1](#) [11]'ine bir göz atın.
- Bilgisayarınızdaki bütün dosyaları düzenli olarak tarayın. Bunu her gün yapmak zorunda değilsiniz (özellikle anti-virüs yazılımınızın, yukarıda anlatıldığı gibi, 'daima açık' özelliği varsa) ama bunu zaman zaman yapmalısınız. Bunu hangi sıklıkta yapmanız gerektiği, içinde bulunduğunuz koşullara bağlıdır. Yakın geçmişte bilgisayarınızla bilmediğiniz bir ağa bağlandınız mı? USB belleklerinizi kimlerle paylaşıyorsunuz? E-postalar vasıtasıyla sık sık bilinmeyen yabancı ekler alıyor musunuz? Evinizdeki ya da iş yerinizdeki biri yakın zamanda virüs sorunu yaşadı mı? Dosyaları en iyi şekilde taramak konusunda daha fazla bilgi için, bakınız: [Avast Rehberi](#) [9].

Virüs bulaşmalarını engellemek

- E-posta eklerini ve anlık mesajlaşma programlarından (MSN, Skype gibi) aldığınız ya da internetten indirdiğiniz dosyaları açarken son derece dikkatli olun. Bilinmeyen bir kaynaktan alınan herhangi bir dosyayı açmaktan kaçınmak en iyisidir. İlla ki bu dosyaları açmanız gerekliyse, dosya ekini ilk önce bilgisayarınızdaki bir klasöre kopyalamalısınız daha sonra (Microsoft Word ya da Adobe Acrobat gibi) uygun bir uygulamayla kendiniz açmalısınız. Dosyaya çift tıklamak ya da e-posta programınızın dosyayı otomatik olarak açmasına izin vermek yerine, programın dosya menüsünü kendiniz elle açmak için kullanırsanız, virüse temas etmeniz daha az olasıdır.
- CD, DVD, USB bellekler gibi çıkarılabilir medyaları bilgisayarınıza takmadan önce olası riskleri göz önünde bulundurun. Anti-virüs programınızın son güncellemelere sahip ve tarayıcısının çalışıyor olduğundan emin olun. Virüsler tarafından bilgisayarınıza bulaşmak için kullanılabilecek olan işletim sisteminizin 'Otomatik Çalıştır/AutoPlay' özelliğini devre dışı bırakmak iyi bir fikirdir. Bu, Windows XP altında [Bilgisayarım](#)'a giderek, CD ya da DVD sürücünüze farenizin sağ tuşuyla tıklayarak, [Özellikler](#)'i seçerek ve [Otomatik Çalıştır](#) sekmesine tıklayarak yapılabilir. Her içerik türü için [Eylem yürütme](#) ya da [Her defasında eylem seçmemi](#) iste seçeneklerini seçin ardından da [Tamam](#)'a tıklayın.
- Virüs bulaşmalarının yayılmasını engellemenin bir yolu da , ücretsiz ve açık kaynak kodlu yazılımlara geçmektir. Bu yazılımlar, çoğu zaman daha güvenli olan ve virüs yazarlarının hedef alma olasılığı daha düşük olan yazılımlardır.

Assani: Bir virüs temizleyicim var ve düzenli olarak onu çalıştırıyorum. Bu, bilgisayarımın sağlıklı olduğu anlamına gelir,

değil mi?

Salima: Doğrusu bir anti-virüs programına sahip olmak yeterli değildir. Bilgisayarını casus yazılımlara ve hacker'lara karşı da korumalısın, bu nedenle birkaç araç daha yüklemek zorundasın.

Casus yazılım

Casus yazılımlar hem bilgisayarınızda hem de internette yaptığınız işleri takip etme ve bunlar hakkında erişimi olmaması gereken kişilere bilgi gönderme yetisine sahip, kötü amaçlı yazılımlar kategorisi altında tanımlayabileceğimiz bir yazılım türüdür. Bu programlar, diğer şeylerin yanı sıra, klavyenizle yazdığınız sözcükleri, farenizin hareketlerini, ziyaret ettiğiniz internet sayfalarını ve çalıştırdığınız programları kaydedebilir. Sonuç olarak bilgisayar güvenliğinizi yavaş yavaş yok edebilir ve sizin, aktiviteleriniz ve bağlantılı olduğunuz kişiler hakkında gizli bilgileri ifşa edebilir. Casus yazılımlar, virüslerle neredeyse aynı şekilde bilgisayarlara bulaşır. Bu nedenle, yukarıdaki tavsiyelerin birçoğu bu ikinci tür kötü amaçlı yazılımlara ^[2] karşı bilgisayarınızı korumak için de faydalıdır. Kötü amaçlı web sayfaları casus yazılım bulaşmasının belli başlı kaynaklarından biri olduğundan, ziyaret ettiğiniz web sayfalarına daha da dikkat etmelisiniz ve tarayıcınızın ayarlarının güvenli olduğundan emin olmalısınız.

Assani: Bu anlatılanların hepsi kulağa casus filmlerinden fırlamış senaryolar gibi geliyor. Bilgisayarına gerçekten de "casus yazılımlar bulaşmış" olabilir mi?

Muhindo: İster inan ister inanma, bu çok yaygın bir durum. İnternette indirdiğin programlar bilgisayarına casus yazılım bulaştırmamışsa bile ziyaret ettiğin web sayfalarından en az birinin bulaştırmış olma ihtimali yüksektir. Windows ve Internet Explorer kullanıyor olman bu olasılığı daha da yükseltiyor. Bilgisayarını casus yazılımlar için hiçbir zaman taratmadıysan, eminim ki şimdiye dek ne kadar çok casus yazılımın bilgisayarına kurulduğunu gördüğünde şaşıracaksın.

Anti-Casus yazılımlar

Anti-casus yazılım araçlarını, bilgisayarınızı bu tür tehditlere karşı korumak için kullanabilirsiniz. Spybot ^[4] bu tür programlardan biridir ve anti-virüs programlarının görmezden geldiği belirli türden kötü amaçlı yazılımların tanımlanması ve silinmesinde oldukça başarılı bir araçtır. Tıpkı anti-virüs yazılımlarında olduğu gibi Spybot'un kötü amaçlı yazılım ^[2] tanımlarını güncellemeniz ve düzenli taramalar yapmanız çok önemlidir.

Uygulama: Spybot - Anti-Casus Yazılım Rehberi ^[12] ile uygulamaya başlayın.

Casus yazılım bulaşmasını önlemek

- Web sitelerini tararken tedbirli olun. Otomatik olarak beliren tarayıcı pencerelerini izleyin ve **Evet** ya da **Tamam**'a tıklamadan önce onları dikkatle okuyun. Şüpheli durumlarda, 'kendiliğinden açılan pencereleri' kapatmak için **İptal**'e tıklamak yerine, sağ üst köşedeki **X**'e tıklayarak kapatmalısınız. Bu, web sitelerinin isteminiz dışında bilgisayarınıza kötü amaçlı yazılım yüklemenize neden olacak hilelerini önlemeye yardımcı olabilir.
- Web tarayıcınızın güvenliğini, bazen ziyaret ettiğiniz sayfaların içinde yer alan potansiyel olarak tehlikeli programları otomatik olarak çalıştırmasını engelleyerek artırabilirsiniz. Mozilla Firefox ^[13] kullanıyorsanız, Firefox Rehberi ^[14]'nin 4. Bölüm ^[15]'ünde anlatıldığı gibi, NoScript ^[16] eklentisini kurabilirsiniz.
- Bilmediğiniz ya da güvenmediğiniz web sitelerinden gelen bu tür içerikleri asla kabul etmeyin ve çalıştırmayın.

Assani: 'Java applet'lerin ve 'ActiveX control'lerin tehlikeli olduğunu duydum. Ama onların ne olduğu konusunda bir fikrim yok.

Salima: Bunlar sadece aynı türden şeylerin farklı örnekleridir: Web tarayıcısının okumakta olduğu sayfayla birlikte kimi zaman indirdiği küçük programlardır. Web tasarımcıları karmaşık web siteleri yaratmak için bunları kullanır, ama bunlar virüs ve casus yazılım yaymak için de kullanılabilir. NoScript kurduysan ve düzenli olarak çalıştırıyorsan bunların gerçekte nasıl çalıştığı konusunda endişelenmene gerek yok.

Güvenlik duvarı

Bir güvenlik duvarı internette gelen veriyi bir bilgisayarda ilk gören programdır. Ayrıca dışarı gönderilen bilgiyi ele alan en son programdır. Bir binanın girişine konumlanmış, kimin girip kimin çıkabileceğine karar veren bir güvenlik görevlisi gibi, bir güvenlik duvarı gelen ve giden verileri alır, inceler ve onlar hakkında karar verir. Doğal olarak, hacker'lara ve virüslere bilgisayarınıza erişim için açık bir yol sağlamamak için, internette ve yerel ağlardan güvenmediğiniz bağlantılara karşı kendinizi savunmanız yaşamsal önemdedir. Doğrusu, bilgisayarınızın dışa doğru bağlantılarını izlemek de aynı derecede önemlidir.

İyi bir güvenlik duvarı bilgisayarınızdaki her programın erişim izinlerini seçmenize izin verir. Bu programlardan biri dış dünyayla bağlantı kurmaya çalıştığında, güvenlik duvarınız, programı tanıdığı ve bu tür bağlantılar için ona izin verdiğinizi doğrulayabildiği durumlar hariç, girişimi engelleyecek ve size bir uyarı verecektir. Bu büyük ölçüde var olan kötü amaçlı yazılımların ^[2] virüs yaymasını ya da bilgisayarınıza hacker'ları davet etmesini engellemek içindir. Bu açıdan bir güvenlik duvarı, hem ikinci bir savunma hattı hem de bilgisayarınızın güvenliğinin tehdit edildiğini anlamanıza yardım edebilecek bir erken uyarı sistemi sağlar.

Güvenlik Duvarı Yazılımı

Microsoft Windows'un son sürümleri şimdilerde otomatik olarak açılan yerleşik güvenlik duvarı içeriyor. Ne yazık ki Windows güvenlik duvarı birçok açıdan sınırlıdır, örneğin, dışa dönük bağlantıları incelemeyi. Ancak bilgisayarınızı güvenli tutmak konusunda daha başarılı bir program olan [Comodo Personal Firewall](#) ^[5] adlı mükemmel bir [ücretsiz yazılım](#) ^[8] programı bulunmaktadır.

Uygulama: [Comodo Firewall Rehberi](#) ^[17] ile uygulamaya başlayın

Güvenilmez ağ bağlantılarını engellemek

- Hassas işler için kullanacağınız bilgisayara sadece önemli programları kurun ve onları güvenilir kaynaklardan edindiğinizden emin olun. Kullanmadığınız herhangi bir programı ise kaldırın.
- Kullanmadığınız zamanlarda bilgisayarınızın internet bağlantısını kapatın ve geceleri bilgisayarınızı tamamen kapatın.
- Windows şifrenizi kimseyle paylaşmayın.
- Kullanmadığınız 'Windows hizmetlerini' açtıysanız onları kapatmanız gerekir. Bu konuda daha fazla bilgi için [Okuma önerileri](#) ^[18] ne bakınız.
- Çalıştığınız yerdeki tüm bilgisayarlarda bir güvenlik duvarının kurulu olduğundan emin olun
- Kurulu güvenlik duvarı yoksa, çalıştığınız yerdeki bütün yerel ağı korumak için ek bir güvenlik duvarı kurmayı düşünmelisiniz. Birçok ticari geniş bant [ağ geçitleri](#) ^[19] kullanması kolay bir güvenlik duvarı içerir, ve onu çalışır hale getirmek ağınıza çok daha güvenli kılabilir. Bu konuda nereden başlayacağınızı bilmiyorsanız, ağınıza kurmaya yardım eden kişilerden destek isteyebilirsiniz.

Asani: Demek ki sen benden anti-virüs, anti-casus yazılım ve güvenlik duvarı yazılımları kurmamı istiyorsun? Bilgisayarım bütün bunlarla baş edebilir mi?

Muhindo: Kesinlikle. Doğrusu bu üç araç, bugünlerde internette güvenli kalmak için asgari olmazsa olmaz programlardır. Bu programlar birlikte çalışacak şekilde tasarlanmıştır, öyle ki bunların tümünü kurmanın hiçbir sorun çıkarmaması gerekir. Yine de iki anti-virüs programını ya da iki güvenlik duvarını aynı anda çalıştırmak istememen gerektiğini hatırlamalısın.

Yazılımlarınızı güncel tutmak

Bilgisayar programları çoğu zaman büyük boyutlu ve karmaşıktır. Düzenli olarak kullandığınız yazılımlardan bazılarının keşfedilmemiş hatalar içermesi kaçınılmazdır ve bu hatalardan bazılarının bilgisayarınızın güvenliğini tehlikeye atması olasıdır. Yazılım tasarımcıları bu hataları bulmaya ve bunları onarmak için güncellemeler çıkarmaya devam etmektedir. **Bu nedenle bilgisayarınızdaki işletim sistemi dâhil, bütün yazılımları sık sık güncellemeniz çok önemlidir.** Windows otomatik olarak kendisini güncellemezse, **Başlat** menüsüne tıklayarak, **Tüm Programları** ve ardından **Windows Update**'i seçerek, Windows'u düzenleyebilirsiniz. Bu, Internet Explorer'ı açacak ve sizi **Otomatik Güncelleme** özelliğini etkinleştirebileceğiniz Microsoft Update sayfasına götürecektir. Bu konuda daha fazla bilgi için [Okuma önerileri](#) ^[18] ne bakınız.

Benzer bir şekilde bilgisayarınızdaki kurulmuş tüm diğer programların da güncel olduğundan emin olmanız önemlidir. Bunu yapabilmek için öncelikle bilgisayarınızda hangi programların olduğunu bilmeniz ve belki de önemli olmayanları kaldırmanız gerekir (Windows'da Denetim Masası'na gidin ve *Programlar* ardından *Program Ekle/Kaldır*). Ardından da her programın son versiyonu olup olmadığını, nasıl güncellendiğini ve ileride otomatik olarak kendi kendini güncelleyip güncellemeyeceğini gözden geçirmek iyi olacaktır.

Ücretsiz yazılımlar ve FOSS (ücretsiz ve açık kaynak kodlu yazılım) araçlarıyla güncel olmak

[Sahipli yazılımlar](#) ^[20] güncellemeleri kurmanıza izin vermeden önce, yazılımın yasal olarak satın alındığına dair bir kanıt istemektedir. Örneğin, Microsoft Windows'un korsan bir kopyasını kullanıyorsanız kendi kendisini güncelleyemeyebilir. Bu da sizi ve bilgilerinizi micro derece saldırıya açık hale getirebilir. Geçerli bir lisans olmaksızın, kendinizi ve diğerlerinizi riske atarsınız. Yasa dışı yazılımlara güvenmek, teknik olmayan riskler de oluşturabilir. Sayısı her geçen gün artan pek çok ülkedeki yetkililer, kullanılan her bir yazılım için kuruluşların geçerli bir lisansa sahip olduğunu doğrulamaya başladı. Polis bilgisayarlara el koydu ve 'yazılım korsanlığı' gerekçesiyle kuruluşları kapattı. Bu mantık, verili kuruluşların çalışmalarına müdahale etmek için siyasi gerekçeleri olan otoritelerin ülkelerinde kolayca kötüye kullanılabilir. Neyse ki bu tür taktiklere karşı kendinizi korumak için pahalı yazılımlar satın almak zorunda değilsiniz.

Şu anda kullanmakta olduğunuz [sahipli yazılımlara](#) ^[20], özellikle lisanssız olanlara alternatif olarak [ücretsiz yazılım](#) ^[8] ve [FOSS](#) ^[7] 'ları (ücretsiz ve açık kaynak kodlu yazılım) denemenizi ısrarla tavsiye ediyoruz. [Ücretsiz yazılım](#) ^[8] ve [FOSS](#) ^[7] araçları çoğu zaman gönüllüler ya da kâr amacı gütmeyen örgütler tarafından ücretsiz olarak yazılır, piyasaya sürülür ve hatta güncellenir. Özellikle [FOSS](#) ^[7] araçlarının, [sahiplilere](#) ^[20] göre daha güvenli oldukları düşünülür çünkü farklı uzman grupları, sorunu tanımlayabilecek ve çözüme katkıda bulunabilecek herhangi bir kimse tarafından, [kaynak kodlarının](#) ^[21] incelenmesine izin verecek şekilde, şeffaf olarak üretilirler.

Birçok [FOSS](#) ^[7] uygulaması, yerini tutmak üzere yazılan sahipli yazılımlar gibi görünür ve onlara benzer bir şekilde çalışır. Aynı zamanda bu programları, Windows işletim sistemi de dahil olmak üzere diğer sahipli yazılımlarla birlikte sorunsuz olarak kullanabilirsiniz. Meslektaşlarınız belirli türden bir programın ticari sürümünü kullanmaya devam etse bile onlarla hâlâ dosya değiş tokuş edebilir ve kolayca bilgi paylaşabilirsiniz. Özellikle Internet Explorer'ı, Outlook'u ya da Outlook Express'i ve Microsoft Office'i sırasıyla Firefox'la, Thunderbird'le ve [LibreOffice](#) ^[22] 'le değiştirmeyi düşünmelisiniz.

Aslında Microsoft Windows işletim sisteminden bile tamamen uzaklaşabilir ve [GNU/Linux](#) [6] olarak adlandırılan daha güvenli [FOSS](#) [7] alternatifini kullanmayı deneyebilirsiniz. Değişimi gerçekleştirmeye hazır olup olmadığınızı anlamanın en iyi yolu basitçe denemektir. [Ubuntu Linux](#) [23]'ün bir [LiveCD](#) [24] sürümünü indirebilir, bir CD ya da DVD'ye yazabilir ve bilgisayarınıza takıp onu yeniden başlatabilirsiniz. Yükleme tamamlandığında bilgisayarınız [GNU/Linux](#) [6] çalıştıracaktır ve ne düşündüğünüze karar verebilirsiniz. Endişelenmeyin, bunlardan hiçbirisi kalıcı değildir. Bitirdiğinizde basitçe bilgisayarınızı kapatın ve Ubuntu [LiveCD](#) [24]'yi çıkarın. Bilgisayarınızı yeniden başlattığınızda, Windows'a geri dönmüş olacaksınız ve diğer uygulamalarınızı, ayarlarınızı ve verilerinizi aynen bıraktığınız gibi bulacaksınız. Açık kaynak kodlu yazılımın genel güvenlik avantajlarına ek olarak Ubuntu'nun, işletim sisteminizi ve diğer birçok yazılımınızı eski ve güvencesiz olmaktan koruyacak, ücretsiz ve kullanımı kolay bir güncelleme aracı vardır.

Okuma önerileri

- Bakınız: [Digital Security and Privacy for Human Rights Defenders](#) [25] kitabının *Malicious Software and Spam* bölümü ve *Internet Program Settings* eki.
- Yeni virüslerle ilgili haberlere güncel kalmak için [Virus Bulletin](#) [26] web sitesine göz atın.
- Gereksiz olan 'Windows hizmetleri'ni nasıl tespit edebileceğinizi öğrenin ve [ihtiyacınız olmayanları etkisiz kılın](#) [27].
- [Tactical Technology Collective](#) [28]'in diğer alet takımları, yazılımınızın ihtiyacı olan FOSS ve Ücretsiz yazılım araçlarını kullanıma açmanız için size yardımcı olabilir.
- Bilgisayarınızda Windows'u başlatmadan önce bilgisayarınızı taramak ve virüsleri temizlemek için [Ücretsiz önyüklenabilir kurtarma CD'lerini indirin](#) [29].
- Bilgisayarınıza virüs ya da başka bir kötü amaçlı yazılım bulaştığını düşünüyorsanız [Malware Removal Guide for Windows](#) [30]'u okuyunuz.

2. Fiziksel tehditlere karşı bilgilerinizi nasıl korursunuz

Bilgisayarınızın çevresinde dijital bir bariyer kurmak için ne kadar çaba sarf ederseniz edin, bir sabah uyandığınızda, bilgisayarınızın ya da bilgisayarınızdaki bilgilerin bir kopyasının kaybolduğunu, çalındığını ya da talihsiz kazalar veya kötü niyetli hareketler sonucu zarar gördüğünü fark edebilirsiniz. Elektrik dalgalanması, açık bir pencere ya da bir fincan kahvenin dökülmesi gibi pek çok şey, tüm verilerinizin kaybolduğu ve bilgisayarınızı kullanmanızın mümkün olmadığı bir duruma yol açabilir. Dikkatli bir risk analizi, sağlıklı bir bilgisayar ortamını sürdürmek için tutarlı bir çaba ve yazılı bir [güvenlik politikası](#) [31] bu tür felaketlerden kaçınmaya yardım edebilir.

Arka plan senaryosu

Shingai ve Rudo Zimbabwe'nin HIV-pozitif nüfusunun uygun ilaçlara erişimine yardım etmek için uzun yıllardır çalışan yaşlı bir evli çifttir. Ofislerine yeni bilgisayarlar ve internet araç-gereçleri almak için bir hibe programına başvurumaktadırlar. Hem altyapısal olarak hem de politik anlamda karışık bir bölgede yaşadıklarından, onlar ve onların potansiyel mâli destekçileri yeni donanımlarının sadece hacker'lar ve virüslere karşı değil; aynı zamanda el koymalara, fırtınalara, ani elektrik yükselişleri ve diğer benzeri felaketlere karşı da güvenliğinin sağlanmasını istemektedir. Bu nedenle Shingai ve Rudo, hibe başvuruları başarılı olursa almayı planladıkları bilgisayarların ve ağ donanımlarının fiziksel güvenliğini artırmak için bir plan geliştirmek üzere yerel bir bilgisayar teknisyeni olan Otto'dan yardım istediler.

Bu bölümden ne öğrenebilirsiniz

- Bilgisayarınıza ve bilgisayarınızın içinde depolanmış bilgiye yönelik [fiziksel tehditlerden](#) [32] birkaçı hakkında daha fazlasını
- Bu tehditlere karşı bilgisayar malzemelerinin en iyi şekilde nasıl güvence altına alınacağı
- Bilgisayarlar ve ağ donanımları için sağlıklı bir işletim ortamının nasıl yaratılacağı
- Ofisinizdeki bilgisayarlar için bir güvenlik planı oluştururken neleri göz önünde bulundurmak gerektiği

Risklerinizi değerlendirmek

Birçok kuruluş, ofislerinin ve malzemelerinin fiziksel güvenliğini korumanın önemini küçümsemektedir. Sonuç olarak çoğu zaman, bilgisayarlarını ve yedek depolama araçlarını hırsızlığa, şiddetli hava koşullarına, kazalara ve diğer [fiziksel tehditlere](#) [33] karşı korumak için almaları gereken önlemleri içeren açık bir politikadan yoksundurlar. Bu tür politikaların öneminin malum olduğu düşünülebilir ancak bu politikaları düzgün bir şekilde formüle etmek görüldüğünden daha zor olabilir. Örneğin birçok kuruluş, ofislerinin kapısında kaliteli kilidlere sahip olabilir ve hatta birçoğu güvenli pencerelere sahip olabilir; ama yaptıkları anahtar sayısına ve bu anahtarların kopyalarına sahip olanlara dikkat etmezlerse sahip oldukları hassas bilgiler saldırıya açık hale gelebilir.

Shingai: Güvenlik politikamızın kısa bir özetini bu hibe başvurusuna koymak istiyoruz ama aynı zamanda bu politikanın kapsayıcı olduğundan da emin olmak istiyoruz. Buna ne eklememiz gerekir?

Otto: Maalesef fiziksel tehditlere karşı her duruma uyan tek bir çözüm tavsiye edemem. İyi bir politikanın özelliği, neredeyse her zaman, belirli bir kuruluşun özgün koşullarına bağlı olmasıdır. Yine de size genel bir tavsiye: Bir plan oluşturmaya çalıştığınızda çalışma ortamınızı dikkatlice gözlemlemeniz; zayıf noktalarınızın nerelerde olduğunu tespit etmeniz ve bunları güçlendirmek için neler yapabileceğinizi yaratıcı bir biçimde düşünmeniz gerekir.

Sizin ve kuruluşunuzun karşılaştığı riskleri ve saldırıya açık noktaları değerlendirirken verilerinizin tehdit edildiği birçok farklı düzeyi değerlendirmeniz gerekir.

- Kullandığınız iletişim kanallarını ve onları nasıl kullandığınızı göz önünde bulundurun. Örneğin; basılı mektuplar, faksler, sabit hatlı telefonlar ve cep telefonları, e-postalar ve [Skype](#) [34] mesajları gibi...
- Önemli bilgileri nasıl depoladığınızı düşünün. Bilgisayar sürücüler, e-posta ve ağ sunucuları, USB bellekler, USB harici sürücüler, CD'ler ve DVD'ler, cep telefonları, basılı ya da elle yazılmış notlar gibi...
- Bu nesnelerin fiziksel olarak nerede konumlandığını göz önünde bulundurun. Ofiste, evde, çöp sepetinde ya da 'internette bir yerlerde'. Bu son durumda belirli bir bilgi parçasının gerçek, fiziksel konumunu belirlemek oldukça zor olabilir.

Aynı bilgi parçasının birçok farklı düzeyden saldırıya açık olabileceğini aklınızda bulundurun. [Kötü amaçlı yazılımlara](#) [2] karşı USB belleklerin içeriğini korumak için bir anti-virüs yazılımına güvenmek zorunda olduğunuz gibi, aynı bilgiyi; çalınmaya, kaybolmaya ya da tahrip olmaya karşı korumak için ayrıntılı bir güvenlik planına güvenmek zorundasınız. Bazı güvenlik uygulamalarına sahip olmak, (örneğin ortam-dışı yedekleme politikasına sahip olmak gibi) hem dijital hem de fiziksel tehditlere karşı yardımcı olsa da bazı diğer güvenlik uygulamaları daha spesifik amaçlar için hazırlanmıştır.

USB belleklerinizi cebinizde mi yoksa bavulunuzun dibindeki kilitli bir plastik çantada mı taşıyacağınıza karar verdiğinizde, her ne kadar korumaya çalıştığınız bilgi dijitalse de, fiziksel güvenlik hakkında bir karar vermektedirsiniz. Her zaman olduğu gibi doğru bir güvenlik politikası büyük oranda içinde bulunulan duruma bağlıdır. Şehir içinde mi yürüyorsunuz yoksa sınır ötesine mi seyahat edeceksiniz? Çantanızı bir başkası mı taşıyacak? Yağmur yağıyor mu? Bu tür kararları verirken göz önünde bulundurmanız gereken sorular bunlardır.

Fiziki saldırganlara karşı bilgilerinizi korumak

Hassas bilgilerinize erişmeye çalışan kötü niyetli kişiler [fiziksel tehditlerin](#) [33] önemli bir türünü temsil eder. Bilgilerinizin güvenliğine karşı var olan tek tehdidin bu olduğunu varsaymak hatadır ama bunu görmezden gelmek daha da büyük bir öngörüsüzlük olur. Fiziksel saldırı riskini azaltmaya yardım etmek için atabileceğiniz bir dizi adım vardır. Evinizde olduğu kadar iş yerinizde de uygulayabileceğiniz, aşağıda yer alan kategoriler ve öneriler, kendi özgül fiziksel güvenlik durumunuza uygun olarak üzerine inşa etmeniz gereken bir temeli temsil eder.

İş yerinizin çevresi

- Komşularınızla tanışın. Ülkenizdeki ve yaşadığınız bölgedeki güvenlik durumuna bağlı olarak bir ya da iki şey mümkün olabilir. Ya komşularınızı ofisinize göz kulak olacak müttefiklere dönüştüreceksiniz ya da onları güvenlik planınızda yer vermeniz gereken potansiyel tehlikeler listesine alacaksınız.
- Ofisinize erişimi sağlayan tüm kapıları, pencereleri ve diğer giriş noktalarını nasıl koruyacağınızı gözden geçirin.
- Güvenlik kamerası ya da hareket algılayıcı bir alarm sistemi kurmayı düşünün.
- Ziyaretçilerinizin ofisinize girmeden önce karşılanabildiği bir resepsiyon bölgesi ve olağan çalışma alanınızdan ayrı bir toplantı odası oluşturmaya çalışın.

Ofisinizin içinde

- Ağ kablolarınızı ofisinizin içinden geçirerek koruma altına alın.
- [Sunucular](#) [35], [yönlendiriciler \(router\)](#) [19], [anahtarlar \(switches\)](#) [19], [hub'lar](#) [19] ve modemler gibi ağ araçlarınızı güvenli odalarda ya da dolaplarda kilit altında bulundurun. Bu tür malzemelere fiziksel erişimi olan davetsiz bir misafir, aktarım sırasında verileri çalmaya ya da ofisinizi terk ettikten sonra bile ağınıza bağlı bilgisayarlara saldırıya muktedir bir [kötü amaçlı yazılım](#) [2] kurabilir. Bazı durumlarda sunucularınızı, bilgisayarlarınızı ya da diğer araç gereçlerinizi tavan arasında, sahte bir tavanda ya da hatta bir komşunuzda saklamanız ve onları kablolu bağlantılarla kullanmanız yararlı olabilir.
- Kablolu ağı varsa, saldırganların ağınıza girememesi ya da ağ trafiğinizi izleyememesi için [erişim noktanızı](#) [19] güvenli kılmanız can alıcı önemdedir. Güvensiz bir kablolu ağ kullanıyorsanız mahallenizde dizüstü bilgisayar olan herkes potansiyel bir tehdittir. Bu 'fiziksel'in sıradışı bir tanımıdır ancak kablolu ağınıza izleyen kötü niyetli kişilerin, ofisinize sızıp ethernet kablolarından bağlanan kişilerle aynı erişime sahip olduğunu göz önünde bulundurmanız yardımcı olur. Kablolu ağınıza güvenli kılmak için gerekli adımlar, [erişim noktanızdaki](#) [19] donanım ve yazılımlara bağlı olarak çeşitlilik gösterecektir ama bu adımları atmak çoğunlukla güç değildir.

İşinizin başındayken

- Bilgisayar ekranınızı, hem masanızın başındayken hem de siz ofisinizin dışındayken, ekranda sergilenenlerin okunmasını engelleyecek şekilde, dikkatli bir biçimde konumlandırılmalıdır. Bu, ofisinizdeki pencerelerin, açık kapıların ve varsa konuk bekleme alanınızın konumunu gözden geçirmeniz gerektiği anlamına gelir.
- Birçok masaüstü bilgisayar kasası, anahtarı olmayanların içeri girmesini engelleyecek, asma kilit takabileceğiniz bir

deliğe sahiptir. Ofisinizde buna benzer bilgisayar kasaları varsa saldırganların dahili donanımlara zarar vermesini engellemek için bunları kilitlemelisiniz. Yeni bilgisayar satın alırken de bu özelliği göz önünde bulundurun.

- Olanaklı olduğu yerlerde, saldırganların bilgisayarların kendisini çalmasını engellemek için kilitli bir güvenlik kablosu ^[36] kullanın. Bu özellikler, bir çantanın içinde ya da paltonun altında gizlenebilecek dizüstü ve küçük masaüstü bilgisayarlar için önemlidir.

Yazılım ve ayarlarla ilgili fiziksel güvenlik

- Bilgisayarınızı başlattığınızda, bilgisayarınızın bir yazılımı çalıştırmanıza ya da dosyalarınıza erişiminize izin vermeden önce bir şifre sorduğundan emin olun. Sormuyorsa, bu özelliği Windows'da *Başlangıç* menüsünden Denetim Masası'nı ve Kullanıcı Hesapları'nı çift tıklayarak etkin hale getirebilirsiniz. Kullanıcı Hesapları ekranında, kendi hesabınızı seçin ve Hesabınız için bir Parola Oluşturun'a tıklayın. **3. Bölüm: Güvenli şifreler nasıl oluşturulur ve muhafaza edilir** ^[37]'de ele alındığı gibi güvenli bir şifre seçin; şifrenizi girin ve doğrulayın, Parola Oluştur'a tıklayın ve ardından da Evet, Gizli Kılın'a tıklayın.
- Bilgisayarınızın *BIOS* ^[38]'unda fiziksel güvenlikle ilgili bazı ayarlar vardır. İlk olarak, bilgisayarınızı USB cihazlardan, CD-ROM ya da DVD sürücülerinden *başlat* ^[39]ılamayacak şekilde yapılandırılmalısınız. İkinci olarak, davetsiz bir misafirin önceki ayarı basitçe geri almasını engellemek için, *BIOS* ^[38]'un kendisine de bir şifre kurtmalısınız. Tekrar edelim, güvenli bir şifre seçtiğinizden emin olun.
- **3. Bölüm** ^[37]'de tartışıldığı gibi, belirli bir bilgisayar için Windows ya da *BIOS* ^[38] şifrelerini kaydetmek için, şayet güvenli bir şifre veri tabanına güveniyorsanız, veri tabanının sadece tek bir kopyasının o bilgisayarda saklanmadığından emin olun.
- Bilgisayarınızdan uzaklaştığınız zamanlarda hesabınızı kilitlemeyi alışkanlık haline getirin. Windows'da bunu Windows logo tuşunu basılı tutarken L tuşuna basarak hızla yapabilirsiniz. Bu, sadece yukarıda açıklandığı gibi, hesabınız için bir şifre yarattıysanız işleyecektir.
- Bilgisayarlardaki ve depolama aletlerindeki hassas bilgiyi *şifreleyin* ^[40]. İlave detaylar ve uygun Uygulamalı Rehberler'i gösteren işaretçiler için **4. Bölüm: Bilgisayarınızdaki hassas dosyaları nasıl korursunuz** ^[41]'a bakınız.#

Rudo: BIOS'da çalışmak beni biraz endişelendiriyor. Yanlış bir şey yaparsam bilgisayarımı bozabilir miyim?

Otto: Tabii ki bozabilirsin, en azından kısa bir süreliğine. Aslında değiştirmek isteyebileceğin ayarlar oldukça basittir, ama BIOS ekranının kendisi bile biraz korkutucu olabilir, yanlış bir şey yaparsanız bilgisayarınızı geçici olarak çalışamaz hale getirmeniz olasıdır. Genel olarak BIOS'da çalışmaktan rahatsızsanız daha fazla bilgisayar deneyimi olan birinden yardım istemelisiniz.

Taşınabilir cihazlar

- Hassas bilgiler içeren dizüstü bilgisayarınızı, cep telefonunuzu ve diğer taşınabilir cihazlarınızı özellikle seyahat ediyor ya da bir otelde kalıyorsanız daima yanınızda bulundurun. Dizüstü bilgisayar *güvenlik kablosuyla* ^[36] birlikte seyahat etmek, her ne kadar onu takacak uygun bir nesneyi zaman zaman bulmak güç olsa da, iyi bir fikirdir. Unutmayın, yemek zamanları, otel odalarını başıboş bıraktıkları zamanlarda kontrol etmeyi alışkanlık haline getirmiş hırsızlar için en iyi fırsattır.
- Dizüstü bilgisayar, tablet ya da diğer taşınabilir cihazlarınız varsa bunları görünür bir yere koymaktan kaçının. Hırsızlara bu tür değerli donanımlar taşıdığınızı ya da verilerinize erişmek isteyen kişilere omuz çantanızda bilgilerle dolu bir harici disk bulunduğunu sergilemeye gerek yoktur. Taşınabilir cihazınızı açık alanlarda kullanmaktan kaçının ve dizüstü bilgisayarınızı, dizüstü bilgisayar çantasına benzemeyen bir şeyin içinde taşıma fikrini göz önünde bulundurun.

Bilgisayar donanımınız için sağlıklı bir ortam sağlamak

Birçok elektronik cihaz gibi bilgisayarlar da oldukça hassastır. İstikrarsız elektrik kaynaklarına, aşırı sıcaklara, toza, yüksek neme ya da mekanik basınca iyi uyum sağlayamazlar. Bilgisayarınızı ve ağ araçlarını bu tür tehditlerden korumak için yapabileceğiniz bir dizi şey vardır:

- Elektrik akımındaki yükselip alçalmalar ve kesintiler bilgisayarınıza fiziksel bir zarar verebilir. Bu tür düzensizlikler, bilgisayarınızın içerdiği bilgilere zarar vererek ya da elektronik parçalarına fiziksel olarak zarar vererek sabit diskinizi 'çökertebilir'.
 - Maddi durumunuz el veriyorsa çalışma ortamınızdaki önemli bilgisayarlara *Kesintisiz Güç Kaynakları UPS* ^[42] kurtmalısınız. *UPS* ^[42] elektrik arzını düzenler ve elektrik kesintisi durumunda geçici güç sağlar.
 - *UPS* ^[42]'lerin uygun olmadığı ya da çok pahalıya mal olduğu durumlarda, güç dalgalanmalarına karşı hangisi bilgisayarınızı korumaya yardım edecekse, ona göre güç filtreleri ya da regülatörler sağlayabilirsiniz.
 - Önemli aletlerinizi elektrik ağınıza bağlamadan önce onu test edin. 'Toprak hattı' olan elektrik prizlerini kullanmaya çalışın. Ve mümkünse, bilgisayarlarınızı riske atmadan önce, yeni çalışma ortamındaki elektrik sisteminin, lambalar ve fanlar gibi pahalı olmayan araçlara güç verirken nasıl davrandığını görmek için bir ya da iki gün bekleyin.
- Genel olarak kazalara karşı korunmak için, önemli donanımlarınızı koridorlara, resepsiyon alanına ya da diğer

kolayca erişilebilir yerlere koymaktan kaçının. UPS'ler, güç filtreleri, büyük dalgalanmalardan koruyucular, enerji ve uzatma kabloları, özellikle sunuculara ve ağ araçlarına takılmış olanları, kazayla atılan yanlış bir adımla fişten çekilemeyecekleri yerlere konumlandırılmalıdır.

- Kaliteli bilgisayar kabloları, enerji ve uzatma kabloları alabiliyorsanız, tüm ofisinize yetecek kadar ve hatta birkaç tane de fazladan satın almalısınız. Duvar prizlerinden düşen, fişleri güvenli bir şekilde tutamayan ve sık sık kıvılcım çıkaran uzatma kabloları sadece can sıkıcı değil aynı zamanda onlara bağlanan herhangi bir bilgisayarın fiziksel güvenliğine karşı da oldukça zararlıdır. Bunlar, bu durumdan bıkmış kullanıcıların, gevşek bilgisayar kablolarını kısa devre yapan enerji kablolarına bantla bağlamalarına neden olabilirler; bu da açıkça yangın riski yaratır.
- Bilgisayarlarınızdan herhangi birini bir dolabın içinde tutacaksanız, dolabın uygun havalandırmaya sahip olduğundan emin olun, aksi takdirde aşırı ısınabilir.
- Bilgisayar ekipmanları radyatörlerin, ısıtıcıların, klimaların ve diğer hava kanallarının yanına yerleştirilmemelidir.

Kendi fiziksel güvenlik politikanızı oluşturmak

Kendinizin ve kuruluşunuzun karşı karşıya olduğu tehditleri ve zayıf noktaları değerlendirdiğinizde, fiziksel güvenliğinizi arttırmak için hangi adımların atılması gerektiğini düşünmelisiniz. Bu adımları yazılı hale getirerek ayrıntılı bir güvenlik politikası ^[31] yaratmalısınız. Sonuçta ortaya çıkan belge size, meslektaşlarınıza ve kuruluşunuza yeni katılan kişilere genel bir rehber olarak hizmet edecektir. Bu belge çeşitli fiziksel güvenlik acil durumlarında yapılması gerekenlere ilişkin bir liste de sağlayacaktır. İşin içindeki herkes bu güvenlik standartlarını okumak, uygulamak ve korumak için zaman ayırmalı ve bu belgenin nasıl geliştirilebileceğine ilişkin soru sormaya ve öneri sunmaya da teşvik edilmelidir.

Fiziksel güvenlik politikanız ^[31] duruma bağlı olarak birçok bölümü içerebilir:

- Alarm sistemlerine, var olan anahtarlara ve bu anahtarların kimlerde olduğuna, misafirlerin ofise ne zaman kabul edildiğine, temizlik sözleşmesinin kiminle yapıldığına ve bu gibi benzer sorunlara işaret eden, ofise erişim politikası
- Ofisin hangi bölümlerinin ziyaretçiler için ayrılacağına ilişkin bir politika
- Seri numaraları ve fiziksel betimlemeleri de dahil, ekipmanlarınızın kaydı
- Hassas bilgileri içeren kâğıt çöplerinin güvenli ortadan kaldırılması için bir plan
- Aşağıdaki durumlarla ilgili acil durum prosedürleri:
 - Hassas bilgiler açığa çıktığında ya da yanlış konumlandırıldığında kim bilgilendirilecek,
 - Yangın, sel ya da diğer doğal felaketler durumunda kiminle iletişime geçilecek
 - Belirli acil tamirler nasıl yapılacaktır
 - Elektrik enerjisi, su ve internet erişimi gibi hizmetleri sağlayan şirketlerle ya da kurumlarla nasıl bağlantı kurulacaktır
 - Çevrimdışı yedekleme sisteminizden bilgiler nasıl kurtarılacaktır. Daha ayrıntılı yedekleme tavsiyelerini **5. Bölüm: Veri kayıpları nasıl kurtarılır** ^[43]'da bulabilirsiniz.

Güvenlik politikanız ^[31] düzenli olarak gözden geçirilmeli ve son gözden geçirmeden sonra yapılan politika değişikliklerini de yansıtmak şeklinde değiştirilmelidir. Ve elbette, geri kalan önemli verilerinizle beraber güvenlik politikası ^[31] belgenizi de yedeklemeyi unutmayın. Bir güvenlik politikası ^[31] oluşturmak konusunda daha fazla bilgi için **Okuma önerileri** ^[44] kısmına bakınız.

Okuma önerileri

- Riskleri değerlendirme konusunda daha fazla bilgi için, Digital Security and Privacy for Human Rights Defenders ^[25] adlı kitabın 1.2 *Security Awareness* ve 1.3 *Threat Assessment* başlıklı bölümlerine bakınız.
- Bir BIOS şifresi oluşturmak konusunda daha ayrıntılı açıklama için, Digital Security and Privacy for Human Rights Defenders ^[25] adlı kitabın 2.1 *Windows Security* başlıklı bölümüne bakınız.
- Güvenlik politikası konusunda rehber için, Digital Security and Privacy for Human Rights Defenders ^[25] adlı kitabın 4. *Case Study 1* başlıklı bölümüne bakınız.
- Ayrıca bakınız, İnsan Hakları Savunucuları için Protection Manual ^[45] ve Protection Handbook ^[46].

3. Güvenli şifreler nasıl oluşturulur ve muhafaza edilir

Bilgisayarlarımızda oturum açmaktan, e-posta göndermeye; hassas verileri şifrelemekten ^[40], gizlemeye kadar, önemli işlerimizi yerine getirmek için dijital teknolojiyi kullanırken rahat hissetmemizi sağlayan güvenli hizmetlerin birçoğu, bir şifre hatırlamamızı gerektirir. Bu gizli sözcükler, sözcük grupları ya da anlamsız karakterler dizisi, bilgileriniz ve onları izniniz olmaksızın okumak, kopyalamak, değiştirmek ve yok etmek isteyen herhangi biri arasındaki ilk ve çoğu zaman tek engeldir. Birinin şifrelerinizi öğrenmesinin birçok yolu vardır ancak belirli birkaç taktik uygulayarak ve KeepPass ^[47] gibi güvenli şifre veri tabanı ^[48] kullanarak bunların birçoğuna karşı şifrelerinizi koruyabilirsiniz.

Arka plan senaryosu

Mansour ve Magda Arapça konuşulan bir ülkede, insan hakları ihlallerini ve siyasi değişim için kampanyayı anonim olarak bloglarında yayınlayan iki kardeşler. Magda kısa bir süre önce e-posta hesabına giriş yapmayı denedi ve şifresinin değiştirildiğini öğrendi. Şifreyi yeniden kurarak oturum açabildi ama gelen kutusunu açtığında birçok yeni mesajın 'okundu'

olarak işaretlendiğini fark etti. Siyasi olarak motive olmuş bir saldırganın birçok web sitesi hesabında kullandığı şifresini öğrenmiş olmasından şüphelendi. Durumu anlatmak ve endişelerini dile getirmek için daha az bilgisayar bilgisi olan Mansour'la buluştu.

Bu bölümden ne öğrenebilirsiniz

- Güvenli bir şifrenin unsurları
- Uzun ve karmaşık şifreleri hatırlamak için birkaç püf noktası
- Şifreleri hatırlamak yerine onları depolamak için [KeePass](#) ^[47] [güvenli şifre veri tabanını](#) ^[48] nasıl kullanacağınızı

Güvenli şifreleri seçmek ve muhafaza etmek

Genellikle, bir şeyi korumak istediğinizde bir anahtarla onu kilitleirsiniz. Evlerin, arabaların ve bisikletlerin kendi fiziksel kilitleri; korunan dosyaların [şifreleme](#) ^[40] anahtarları; banka kartlarının PIN kodları; ve e-posta hesaplarının şifreleri vardır. Fiziksel ve elektronik bütün bu anahtarların tek bir ortak noktası vardır: Bu anahtarlar başkalarının eline geçtiğinde de kilitledikleri kilitleri açarlar. Gelişmiş güvenlik duvarları, güvenli e-posta hesapları ve [şifrelenmiş](#) ^[40] sürücüler kurabilirsiniz ama şifreniz zayıfsa ve onun yanlış ellere geçmesine izin verirsiniz bunların size bir faydası olmayacaktır.

Güçlü bir şifrenin unsurları

Bir şifre, bir bilgisayar programı için tahmin etmesi güç olmalıdır.

- **Şifreniz uzun olmalı:** Şifre uzadıkça bir bilgisayar programının kabul edilebilir bir zaman diliminde onu tahmin edebilmesi daha az olasıdır. On ya da daha fazla karakter içeren şifreler oluşturmaya çalışmalısınız. Bazı insanlar çoğu zaman 'passphrases' olarak adlandırılan, aralarında boşluk olsun ya da olmasın, birden fazla sözcük içeren şifreler kullanır. Bu kullandığınız program ya da hizmetin yeterince uzun şifreler seçmenize izin verdiği sürece çok iyi bir fikirdir.
- **Şifrenizi karmaşık kılın:** Uzunluğa ek olarak bir şifrenin karmaşıklığı da 'şifre kırıcı' yazılımların karakterlerin doğru kombinasyonunu tahmin etmesini engellemeye yardım eder. Mümkünse şifrenize daima büyük ve küçük harfler, sayılar ve noktalama işaretleri gibi simgeler dahil edin.

Bir şifre başkaları için tahmin etmesi güç olmalıdır.

- **Şifrenizi pratik kılın:** Hatırlayamadığınız için şifrenizi bir yere yazmak zorundaysanız, masanızı açıkça gören; geçici bir süre için evinize, cüzdanınıza ve hatta ofisinizin dışındaki çöp tenekesine erişen herhangi biri karşısında sizi zayıf kılacak tehditlerin yeni bir kategorisiyle yüzyüze kalabilirsiniz. Uzun ve karmaşık ama yine de hatırlanabilir bir şifre düşünmüyorsanız, aşağıda yer alan [Güvenli şifreleri hatırlamak ve kaydetmek](#) ^[49] kısmının yardımı olabilir. Yardımı olmazsa, yine güvenli bir şifre seçin ama şifrenizi [KeePass](#) ^[47] gibi [güvenli bir şifre veri tabanına](#) ^[48] kaydedin. Microsoft Word belgeleri dahil şifre korumalı diğer türden dosyalara bu amaç için güvenilmemelidir. Çünkü bu tür dosyaların şifrelerinin birçoğu internetten ücretsiz olarak edinilebilecek araçlar kullanılarak saniyeler içinde kırılabilir.
- **Şifrenizi kişisel kılmayın:** Şifreniz sizinle kişisel olarak ilişkili olmamalıdır. Adınızla, sosyal güvenlik ve telefon numaranızla, çocuğunuzun ve evcil hayvanınızın adıyla, doğum gününüzle ya da birinin sizin hakkınızda küçük bir araştırma ile öğrenebileceği herhangi bir bilgi üzerinde temellenen bir sözcük ya da sözcük öbeği seçmeyiniz.
- **Şifrenizi sır olarak saklayın:** Kesinlikle gerekmediği sürece şifrenizi kimseyle paylaşmayın. Ve şifrenizi bir arkadaşınız, aile üyeniz ya da bir meslektaşınızla paylaşmak zorundaysanız onu önce geçici bir şifreyle değiştirmelisiniz, ardından şifrenizi kullanmaları bitince onu yeniden değiştirmelisiniz. Çoğu zaman bir şifreyi paylaşmanın alternatif yolları vardır; örneğin erişime gereksinim duyan kişiler için ayrı hesaplar oluşturmak. Şifrenizi sır olarak saklamak, şifrenizi yazarken ya da [güvenli şifre veri tabanından](#) ^[48] şifrenize bakarken kimin omzunuzun üzerinden şifrenizi okuduğuna dikkat etmek anlamına gelir.

Bir şifre birinin onu öğrenmesi durumunda tehlikeyi en aza indirecek şekilde seçilmelidir.

- **Şifrenizi benzersiz kılın:** Aynı şifreyi birden fazla hesap için kullanmaktan kaçının. Aksi halde o şifreyi öğrenen herhangi biri hassas verilerinizden daha fazlasına erişim elde edecektir. Bu, bazı hizmetlerin bir şifrenin kırılmasından göreceli olarak kolay kılmasından dolayı özellikle doğrudur. Örneğin, Windows kullanıcı hesabınız ve Gmail hesabınız için aynı şifreyi kullanıyorsanız bilgisayarınıza fiziksel olarak erişebilen herhangi biri öncekini kırabilir ve öğrendiğini sonrakine erişmek için kullanabilir. Benzer nedenlerden dolayı şifreleri farklı hesaplar arasında dönüşümlü olarak kullanmak da kötü bir fikirdir.
- **Tazelikliğini koruyun:** Şifrenizi düzenli aralıklarla değiştirin tercihen en azından her üç ayda bir. Bazı insanlar belirli şifrelere oldukça bağlanır ve hiçbir zaman değiştirmez. Bu kötü bir fikirdir. Bir şifreyi ne kadar uzun saklarsanız başkalarının onu tahmin etmek için daha fazla fırsatı olur. Ayrıca biri sizin çalınmış şifrenizi, siz farkında olmaksızın, bilgilerinize ve kullandığınız hizmetlere erişmek için kullanabilirse şifrenizi değiştirtinceye kadar bunu yapmaya devam edeceklerdir.

Mansour: Ya başkasına güvenirsem? Sana şifremi söylemem sorun olmaz, değil mi?

Magda: Şifren konusunda bir başkasına güvenmen onların şifrene iyi bakacağı anlamına gelmiyor, değil mi? Şifrenle kötü bir şey yapmayacak olsam da onu bir yere yazabilirim ve kaybedebilirim ya da bunun gibi bir şey. Şu an yaşadığım sorun bunun gibi bir nedenden bile kaynaklanmış olabilir! Dahası bu sadece güven sorunu değil. Şifreni bilen tek kişi sensen, hesabını biri ele geçirirse kimi suçlayacağın konusunda endişelenerken vakit kaybetmen gerekmez. Örneğin şimdi şifremi hiçbir zaman yazmadığım ve kimseyle de paylaşmadığım için birilerinin şifremi tahmin ettiğinden ya da onu 'kırdığı'ndan

eminim.

Güvenli şifreleri hatırlamak ve kaydetmek

Yukarıdaki öneriler listesine bakarak, fotografik belleği olmayan birinin bu uzun, karmaşık ve anlamsız şifreleri bir kenara yazmaksızın nasıl izini kaybetmeyeceğini merak ediyor olabilirsiniz. Her hesap için ayrı bir şifre kullanmanın önemi bunu daha da zor kılıyor. Hatırlaması kolay ama gelişmiş şifre kırıcı programlar kullanan akıllı bir kişinin bile tahmin etmesi güç olan şifreler oluşturmanıza yardım edecek birkaç püf noktası bulunmaktadır. Özel olarak bu amaç için geliştirilmiş olan [KeePass](#) ^[47] gibi bir araç kullanarak şifrelerinizi kaydetme seçeneğiniz de bulunmaktadır.

Güvenli şifreleri hatırlamak

Bir şifre seçerken farklı karakter tipleri seçmek önemlidir. Bu çeşitli şekillerde yapılabilir:

- Büyük harf kullanımını çeşitlendirerek, örneğin: 'My naME is Not MR. MarSter'
- Sayıları ve numaraları birbirinin yerine kullanarak, örneğin: 'a11 w0Rk 4nD N0 p14Y'
- Belirli simgeleri dahil ederek, örneğin: 'c@t(heR1nthery3'
- Farklı dilleri birleştirerek, örneğin: 'Let Them Eat 1e gateaU au ch()colaT'

Bu yöntemlerin her biri aksi halde basit olacak olan şifrelerin karmaşıklığını arttırmaya yardım eder ve şifrenizi ezberleme fikrinden tamamen vazgeçmeksizin güvenli bir şifre seçmenize yardımcı olur. Daha yaygın olan yer değiştirme yöntemlerinin bazıları ('o' yerine sıfır ya da 'a' yerine '@' simgesini kullanmak gibi) uzun zaman önce şifre kırma araçlarına dahil edildi ama bunları kullanmak hâlâ iyi bir fikirdir. Bunlar, bu tür araçların bir şifreyi öğrenmesi için gereken zamanı uzatır ve bu tür araçların kullanılmadığı daha yaygın durumlarda şanslı tahminleri engellemeye yardım eder.

Şifre yaratırken, kısaltmaların kullanımı gibi daha geleneksel bir yöntemden ([mnemonic devices](#) ^[50]) de yararlanılabilir. Bu, uzun sözcük öbeklerinin karmaşık görünümlü sıradan sözcüklere çevrilmesine izin verir:

- 'To be or not to be? That is the question' '2Bon2B?TitQ'a dönüşür
- 'We hold these truths to be self-evident: that all men are created equal' 'WhtT2bs-e:taMac='a dönüşür
- 'Are you happy today?' 'rU:-)2d@y?'e dönüşür

Bunlar sözcükleri ve sözcük öbeklerini, kendiliğinden karmaşık ve ezberlenebilir kılmak için kendi şifreleme yönteminizi geliştirmenize yardım edecek birkaç örnektir.

Şifreyi daha karmaşık kılmak için gösterilecek küçük bir çabanın güvenliğiniz için büyük bir etkisi vardır. Sadece birkaç karakter bile olsa şifrenin uzunluğunu artırmak ya da sayılar ya da özel karakterler eklemek şifrenin kırılmasını daha güç kılar. Aşağıda yer alan tablo bir hacker'ın şifre kombinasyonlarını birbiri ardına deneyerek, karmaşıklığı gitgide artan şifreleri kırmasının ne kadar süreceğine göstermektedir.

Örnek Şifre	Gündelik kullanımdaki bir bilgisayarla kırması için gerekli zaman	Çok hızlı bir bilgisayarla gerekli olan zaman
bananas	Bir günden az	Bir günden az
bananalemonade	2 gün	Bir günden az
BananaLemonade	3 ay, 14 gün	Bir günden az
B4n4n4L3m0n4d3	3 yüzyıl, 40 yıl	1 ay, 26 gün
We Have No Bananas	19151466 yüzyıl	3990 yüzyıl
W3 H4v3 N0 B4n4n45	20210213722742 yüzyıl	4210461192 yüzyıl

Elbette yukarıdaki şifrelerden herhangi birinin kırılması için gerekli zaman, saldırının doğasına ve saldırganın elinin altındaki kaynaklara bağlı olarak çeşitlilik göstermektedir. Dahası şifre kırmak için sürekli yeni yöntemler geliştirilmektedir. Ne olursa olsun bu tablo, karakterleri değiştirmenin, iki sözcük ya da daha da iyisi bir sözcük öbeği kullanmanın şifreleri kırmayı daha güç hale getirdiğini göstermektedir.

Yukarıdaki tablo [Passfault](#) ^[51]'un hesaplamalarına dayanmaktadır. Passfault, şifrenizin gücünü sınavınıza olanak veren birkaç web sitesinden biridir. Bununla beraber bu tür kaynaklar, farklı türden şifrelerin göreceli etkililiğini sergilemek için iyi olsalar da bu sitelere gerçek şifrenizi girmekten kaçınmalısınız.

Şifreleri güvenli olarak kaydetmek

Bir parça yaratıcılık, tüm şifrelerinizi hatırlamanızı sağlayabilirken; bu şifreleri düzenli aralıklarla değiştirme gereksinimi, yaratıcılığınızı hızla tüketmeniz anlamına gelir. Alternatif olarak, birçok hesabınız için rastgele güvenli şifreler oluşturabilirsiniz ve tümünü hatırlama fikrinden tamamen vazgeçebilirsiniz. Şifrelerinizi hatırlamak yerine [KeePass](#) ^[47] gibi taşınabilir, şifrelenmiş [güvenli bir şifre veri tabanına](#) ^[48] bu şifreleri kaydedebilirsiniz.

Uygulama: [KeePass - Güvenli Şifre Depolama Rehberi](#) ^[52] ile uygulamaya başlayın

Elbette bu yöntemi kullanırsanız [KeePass](#) [47] ya da hangi aracı seçerseniz o araç için oldukça güvenli bir şifre oluşturmanız ve bu şifreyi hatırlamanız özellikle önemli hale gelir. Oluşturduğunuz bu 'master' şifre, belirli bir hesabın şifresine ulaşmak istediğiniz her seferinde kullanmanız gereken tek şifredir. Bu yöntem, yukarıdaki tüm önerileri yerine getirmenizi oldukça kolaylaştırır. [KeePass](#) [47] taşınabilir, bu da öncelikli olarak, kullandığınız bilgisayardan uzakta bir şifreye bakmanız gerektiğinde veri tabanını bir USB belleğe yükleyebileceğiniz anlamını gelir.

Her ne kadar çok sayıda hesabı yönetmek zorunda olan herhangi biri için bu en iyi seçenek olsa da bu yöntemi kullanırken birkaç çekinceyi göz önünde bulundurmalısınız. [KeePass](#) [47] veri tabanınızın yedeğini almanız çok önemlidir. Yedekleme stratejileri konusunda [Veri Kayıpları nasıl kurtarılır](#) [43] başlıklı **5. Bölüm** [43]'e bakınız. Veri tabanınızın şifrelenmiş olması, veri tabanınızın bir kopyasını içeren bir USB belleği ya da yedekleme sürücüsünü kaybettiğinizde paniklemek zorunda olmadığınız anlamına gelir.

İkinci başlıca çekince çok daha önemli olabilir. [KeePass](#) [47] master şifrenizi unutursanız şifrenizi ya da veri tabanının içeriğini kurtarmanızın hiçbir yolu yoktur. O halde hem güvenli hem de akılda kalıcı bir master şifre seçtiğinizden emin olun!

Belirli durumlarda bu yöntemin gücü onun zayıflığı haline gelebilir. Birileri sizi KeePass veri tabanı master şifrenizi vermeye zorlarsa, o kişi, bu KeePass veri tabanındaki bütün şifrelerinize erişim elde edecektir. Karşılaşabileceğiniz durum buysa KeePass veri tabanınızı hassas bir dosya olarak ele alabilirsiniz ve onu **4. Bölüm: Bilgisayarınızdaki hassas dosyaları nasıl korursunuz** [41]'da açıkladığımız gibi koruyabilirsiniz. Ayrıca, daha hassas bilgileri koruyan şifreleri içeren ayrı bir KeePass veri tabanı oluşturabilir ve bu veri tabanı için ek önlemler de alabilirsiniz.

Mansour: Bir dakika. KeePass diğer şifrelerini korumak için tek bir master şifre kullanıyorsa bu tüm hesapların için aynı şifreyi kullanmaktan nasıl daha güvenli olabilir? Demek istediğim kötü niyetli biri master şifreni öğrenirse her şeye erişim elde eder, doğru mu?

Magda: Bu iyi bir düşünce. Master şifreni korumanın çok önemli olduğu konusunda haklısın ama birkaç önemli farklılık var. Bunların birincisi, bu kötü niyetli kişinin sadece şifrene değil KeePass veri tabanı dosyana da ihtiyacı olması. Tüm hesapların için aynı şifreyi kullanırsan, sadece senin şifrene gereksinim duyacaktır. Dahası KeePass'ın aşırı güvenli olduğunu biliyoruz, değil mi? Oysa diğer programlar ya da web sitelerinin bu kadar güvenli olup olmadığını bilmiyoruz. Bazıları diğerlerine göre daha güvenli olabilir ve birilerinin zayıf bir web sitesini kırmasını ve ardından da orada öğrendiklerini kullanarak daha güvenli bir hesaba girmek için kullanmasını istemezsin. Üstelik bir şey daha var. KeePass master şifreni değiştirmenizi oldukça kolay kılar.

Okuma önerileri

- Güvenli şifreler hakkında daha fazla bilgi için bakınız: [Digital Security and Privacy for Human rights Defenders](#) [25] kitabının 2.2 *Password Protection* bölümü ve 'How long should my password be?' başlıklı eki.
- Wikipedia'da [Şifreler](#) [53], [Güçlü şifre için rehberler](#) [54] ve [şifre kırma](#) [55] üzerine bilgilendirici makaleler bulabilirsiniz.

4. Bilgisayarınızdaki hassas dosyaları nasıl korursunuz

'Saldırgan' internet üzerinden verilerinizi okumaya ya da değiştirmeye muktedirse, bilgisayarınızdaki ya da taşınabilir depolama aygıtınızdaki bilgilere yetkilendirilmemiş erişim uzaktan gerçekleştirilebilir; ya da fiziksel olarak donanımınız ele geçirilebilir. Kendinizi her iki türden saldırıya karşı, [Bilgisayarınızı kötü amaçlı yazılımlara ve hacker'lara karşı nasıl korursunuz](#) [56] başlıklı **1. Bölüm** [56]'de ve [Fiziksel tehditlere karşı bilgilerinizi nasıl korursunuz](#) [57] başlıklı **2. Bölüm** [57]'de ele alındığı gibi, verilerinizin fiziksel ve ağ güvenliğini geliştirerek koruyabilirsiniz. Birden fazla savunma düzeyini kullanmanız en iyisidir, bu nedenle dosyalarınızın kendilerini de korumalısınız. Böylelikle, diğer güvenlik çabalarınızın yetersiz olduğu ortaya çıkarsa, hassas verilerinizin güvende olma ihtimali korunabilir.

Bu şekilde verilerinizin güvenliğini sağlamaya yönelik tehditler hakkında iki genel yaklaşım bulunmaktadır. **Dosyalarınızı şifreleyebilirsiniz** [40], böylece onları sizden başka herhangi biri için okunmaz kılarınız, ya da saldırıyanın hassas bilgilerinizi bulamayacağını umarak **onları gizleyebilirsiniz**. Her iki yaklaşım için size yardımcı olabilecek araçlar bulunmaktadır. Bunlara dosyalarınızı hem [şifreleyebilecek](#) [40] hem de gizleyebilecek [TrueCrypt](#) [58] adlı bir [FOSS](#) [7] uygulaması da dahildir.

Arka plan senaryosu

Claudia ve Pablo bir Güney Afrika ülkesindeki insan hakları STK'siyle birlikte çalışmaktadır. Son birkaç aylarını bölgedeki ordu tarafından gerçekleştirilen insan hakları ihlalleri hakkında tanıklardan delil ve beyan toplayarak geçirmişlerdir. Bu beyanların kimler tarafından sağlandığına ilişkin ayrıntılar ortaya çıkarsa hem tanıklık eden cesur insanlar hem de bölgedeki örgüt üyeleri tehlikeye atılmış olacaktır. Hâlihazırda bu bilgi STK'nin, Windows XP işletim sistemiyle çalışan bilgisayarındaki bir excel tablosunda saklanmaktadır. Güvenlik konusunda bilinçli olan Claudia verilerin bir yedeğini, iş yerinin uzağında tuttuğu bir CD'ye kaydetmiştir.

Bu bölümden ne öğrenebilirsiniz

- Bilgisayarınızdaki bilgileri nasıl [şifreleyebileceğinizi](#) [40]
- Bilgilerinizi [şifrelenmiş](#) [40] olarak sakladığınızda hangi risklerle karşı karşıya kalabileceğinizi
- Kaybolması ya da çalınması durumunda USB belleklerinizdeki verileri nasıl koruyabileceğinizi

- Fiziksel ya da uzak saldırganlara karşı bilgilerinizi gizlemek için hangi adımları atabileceğinizi

Bilgilerinizi şifrelemek

Pablo: Ama bilgisayarım zaten Windows kullanıcı hesabı şifresiyle korunuyor! Bu yeterince iyi değil mi?

Claudia: Aslında Windows kullanıcı hesabı şifrelerini kırmak genelde oldukça kolaydır. Dahası bilgisayarını bir LiveCD'yle yeniden başlatacak kadar uzun süre ele geçiren herhangi biri, şifre konusunda endişelenmeksiniz verilerini kopyalayabilir. Bilgisayarını bir süre için alıp götürebilirlerse daha da büyük bir sorunun içindesin demektir. Böyle bir durumda endişelenmen gereken sadece Windows şifresi değildir. Microsoft Word ya da Adobe Acrobat şifrelerine de güvenmemelisin.

Bilgilerinizi şifrelemek ^[40], bilgilerinizi kilitli bir kasada tutmak gibidir. Sadece anahtarı olanlar ya da kilidin şifresini bilenler (bu durumda bir şifreleme ^[40] anahtarı ya da şifre) bilgilerinize erişebilir. Bu benzetme, özellikle TrueCrypt ^[58] ve onun gibi araçlar için uygundur. Öyle ki, bu araçlar her seferinde tek bir dosyayı korumak yerine 'şifrelenmiş bölümler' adı verilen güvenli bölümler oluşturur. Bir şifrelenmiş ^[40] bölüme çok sayıda dosyayı koyabilirsiniz ancak bu araçlar bilgisayarınızın ve USB belleğinizin diğer bölümlerinde depolanmış herhangi bir şeyi korumayacaktır.

Uygulama: TrueCrypt - Güvenli Dosya Depolama Rehberi ^[59] ile uygulamaya başlayın

Her ne kadar diğer yazılımlar da benzer güçlü şifreleme ^[40] yöntemleri sağlasa da, TrueCrypt ^[58] bilgi güvenliği stratejinizi tasarlamaya izin veren birçok önemli özelliğe sahiptir. Tüm dosyalarınız, çalıştığınız sırada oluşturulan tüm geçici dosyalarınız, kurduğunuz tüm programlarınız ve tüm Windows işletim sistemi dosyalarınız dahil, **bilgisayarınızın tüm diskini kalıcı olarak şifreleme** olanağı sunar. TrueCrypt taşınabilir depolama aygıtlarındaki şifrelenmiş ^[40] bölümleri de destekler. Aşağıdaki **Hassas bilgilerinizi gizlemek** ^[60] kısmında betimlenen 'inkâr edebilirlik' özelliğini de sunar. Dahası TrueCrypt ücretsiz ve açık kaynak kodlu ^[7] bir programdır.

Pablo: Tamam şimdi beni endişelendirdin. Aynı bilgisayardaki farklı kullanıcılara ne olacak? Bu 'Belgelerim' klasörümdeki dosyaları okuyabilecekleri anlamına mı geliyor?

Claudia: Düşünme biçimin hoşuma gitti! Windows şifren saldırganlardan seni koruyamıyorsa aynı bilgisayarda hesabı olan diğer insanlara karşı seni nasıl koruyacak? 'Belgelerim' klasörün normalde herkese açıktır. Diğer kullanıcıların şifrelenmemiş dosyalarını okumak için zekice bir şey yapmalarına gerek yoktur. Haklısın, klasörlerini 'özel' kılsan bile, bir çeşit şifreleme kullanmadığın sürece güvende değilsin.

Dosya şifrelemeyi güvenle kullanmak için ipuçları

Gizli verileri depolamak hem sizin için hem de birlikte çalıştığınız insanlar için bir risk oluşturabilir. Şifreleme ^[40] bu riski azaltır ama onu ortadan kaldırmaz. Hassas verileri korumanın ilk adımı dolaşımda olan verileri azaltmaktır. Belirli bir dosyayı ya da bir dosyadaki belirli bir bilgi kategorisini depolamak için iyi bir nedeniniz yoksa onu silmelisiniz (bunu güvenli olarak nasıl yapabileceğiniz konusunda daha fazla bilgi için bakınız: **6. Bölüm: Hassas bilgiler nasıl imha edilir** ^[61]). Atılacak ikinci adım ise TrueCrypt ^[58] gibi iyi bir dosya şifreleme ^[40] aracı kullanmaktır.

Claudia: Belki de bu ifadeleri bize veren kişilerin kimliklerini açığa çıkarabilecek ayrıntıları saklamamıza gerçekten de ihtiyacımız yok. Ne düşünüyorsun?

Pablo: Katılıyorum. Bu konuda mümkün olduğunca az şey kaydetmeliyiz. Dahası kesinlikle kaydetmek zorunda olduğumuz kişi ve yer adlarını korumak için basit bir şifreleme düşünmeliyiz.

Kilitli kasa benzetmesine geri dönecek olursak TrueCrypt ^[58] ya da benzer araçları kullanırken aklınızda bulundurmanız gereken birkaç şey vardır. Kasanız ne kadar güçlü olsun kapısını açık bırakırsanız size bir fayda sağlamayacaktır. TrueCrypt ^[58] bölümünüz kullanıma hazır durumdayken (içeriğine eriştiğiniz her seferinde) verileriniz savunmasız olabilir; o halde içindeki dosyaları gerçekten okuduğunuz ve değiştirdiğiniz zamanlar dışında onu kapalı tutmalısınız.

Şifrelenmiş ^[40] bölümlerinizi kullanıma hazır durumda bırakmamanız gerektiğini özellikle hatırlamanız gereken bazı durumlar şunlardır:

- Herhangi bir zaman aralığı için bilgisayarınızdan uzaklaştığınızda şifrelenmiş bölümlerinizin bağlantısını kesin. Bilgisayarınızı gece boyunca çalışır bıraktığınızda, siz uzaktayken hassas bilgilerinizin fiziksel ya da uzak saldırganların erişimine açık bırakılmadığından emin olun.
- Bilgisayarınızı uyku moduna sokmadan önce şifrelenmiş bölümlerinizin bağlantısını kesin. Bu genel olarak dizüstü bilgisayarlarında kullanılan ancak masaüstü bilgisayarlarında da bulunabilecek, hem 'askıya alma' hem de 'uyku modu' özellikleri için geçerlidir.
- Bilgisayarınızı bir başkasına devretmeden önce şifrelenmiş bölümlerinizin bağlantısını kesin. Bir güvenlik noktasından ya da sınır kapısından bir dizüstü bilgisayarı geçirirken tüm şifrelenmiş ^[40] bölümlerin bağlantısını kesmeniz ve bilgisayarınızı tamamen kapatmanız önemlidir.
- Arkadaşlarınızın ya da meslektaşlarınızın dahil güvenmediğiniz harici bir depolama aygıtını ya da USB belleğini bilgisayarınıza takmadan önce şifrelenmiş bölümlerinizin bağlantısını kesin.
- Şifrelenmiş ^[40] bir bölümü bir USB bellekte saklayacaksanız, aygıtı bilgisayardan ayırmanız bölümün bağlantısını hemen kesmez. Dosyalarınızı aceleyle güvence altına almanız gerekirse de bölümü düzgün bir biçimde kaldırmalısınız. Ardından da harici sürücünün ya da belleğin bağlantısını kesmelisiniz ve bilgisayardan ayırmalısınız. Bunları yapmanın en hızlı yolunu buluncaya kadar biraz pratik yapmak isteyebilirsiniz.

TrueCrypt [58] bölümünü bir USB bellekte saklamaya karar verdiyseniz, TrueCrypt [58] programının da bir kopyasını onunla birlikte tutabilirsiniz. Bu, verilerinize bir başkasının bilgisayarından da erişmenizi sağlar. Genel kurallar hâlâ geçerlidir : bilgisayarın kötü amaçlı yazılımlardan [2] arındırılmış olduğu konusunda güveniniz tam değilse şifrenizi girmemeli ve hassas verilerinize erişmemelisiniz.

Hassas bilgilerinizi gizlemek

Evinizde ya da ofisinizde bir kasa bulundurmakla ilgili sorun, cebinizde bir tane bulundurmanın sözünü bile etmeyelim, fazla göze çarpma eğiliminde olmasıdır. Birçok insanın şifreleme [40] kullanarak kendilerini suçlu duruma düşürmek konusunda mantıklı endişeleri vardır. Veri şifrelemenin [40] meşru nedenleri meşru olmayanlarını kat be kat aşıya bile bu tehdidin gerçekliği göz ardı edilemez. Esasında TrueCrypt [58] gibi bir aracı kullanmaktan kaçınmak için iki neden vardır: kendi kendinizi suçlu durumuna düşürme ve en hassas bilgilerinizin konumuna açıkça işaret etme riski.

Kendi kendinizi suçlu durumuna düşürme riskini göz önünde bulundurmamak

Şifreleme [40] birçok ülkede yasa dışıdır ki bu da bu tür bir yazılımı indirmenin, kurmanın ve kullanmanın bir suç olduğu anlamına gelir. Bilgilerinizi, aralarında polis, ordu ya da istihbarat servislerinin de olduğu bir kesim gruptan korumak istiyorsanız, bu yasaları ihlal etmek, etkinliklerinizin araştırılması ya da örgütünüzün yargılanması için bir bahane olarak gösterilebilir. Bu tarz tehditlerin, burada ele alınan araçların yasalılığıyla gerçekte hiçbir ilgisi olmayabilir. Sadece bir şifreleme [40] yazılımıyla ilişkilendirilmeniz, suç işlediğiniz ya da (şifrelenmiş [40] bölümün içinde gerçekte ne olduğundan bahımsız olarak) casusluk yaptığınız gibi suçlamalara maruz kalmanız için yeterli olabilir. Bu nedenledir ki bu tür araçların sizin durumunuza uygun olup olmadığını dikkatle düşünmelisiniz.

Durum buysa birkaç seçeneğiniz bulunmaktadır:

- Veri güvenliği yazılımı kullanmaktan tamamen vazgeçebilirsiniz; bu da sadece gizli olmayan bilgileri saklamanızı ya da hassas dosyalarınızın önemli unsurlarını korumak için bir şifreli sözcük sistemi icat etmenizi gerektirir.
- Hassas bilgilerinizi şifrelemek yerine onları gizlemek için steganografi [62] olarak adlandırılan tekniği kullanabilirsiniz. Bu konuda yardımcı olabilecek araçlar bulunmaktadır ama bunları uygun bir şekilde kullanmak çok dikkatli bir hazırlığı gerektirir ve kullandığınız araçları öğrenen herhangi birinin gözünde kendi kendinizi suçlu duruma düşürme riski hâlâ bulunmaktadır.
- Tüm hassas bilgilerinizi güvenli bir webmail hesabında depolamayı deneyebilirsiniz ama bu güvenli bir ağ bağlantısını ve görece ileri düzey bilgisayar ve internet bağlantısı bilgisini gerektirir. Bu teknik, ağ üzerinden şifrelemenin [40] dosya şifrelemesine [40] göre daha az suç isnad ettiğini ve hassas verileri sabit diskinize kazara kopyalamaktan ve orada bırakmaktan kaçınabileceğinizi varsayar.
- Hassas bilgilerinizi bir USB bellekte ya da harici sabit diskte saklayarak bilgisayarınızdan uzak tutabilirsiniz. Bununla beraber bu tür cihazlar kaybedilmeye ya da el konulmaya daha açıktır; bu nedenle bunlarda hassas, şifrelenmemiş bilgileri taşımak genellikle kötü bir fikirdir.

Gerekliyse bu türden bir dizi taktik kullanabilirsiniz. Bununla beraber, kendi kendinizi suçlu durumuna düşürmekten endişe ettiğiniz durumlarda bile TrueCrypt [58] kullanmak ve şifrelenmiş [40] bölümünüzü olabildiğince gizlemeye çalışmak en güvenli yol olabilir.

Şifrelenmiş bölümünüzü daha az görünür kılmak isterseniz onu farklı bir dosya türü gibi görünecek şekilde yeniden adlandırabilirsiniz. Yaklaşık 700 MB olan geniş bölümleri bir CD imajıymış gibi gizlemek için ".iso" dosya uzantısını kullanmak iyi işleyen bir seçenektir. Daha küçük bölümler için diğer dosya uzantıları daha gerçekçi olabilir. Bu, kasanızı ofisinizin duvarındaki bir tablonun ardına gizlemeye benzer. Sıkı bir aramayı atlatamayabilir ama az da olsa bir koruma sağlar. TrueCrypt [58] programını bir program olarak kurmak yerine onu sabit diskinize ya da USB belleğinize kaydettiğiniz sıradan bir dosya gibi yeniden adlandırabilirsiniz. TrueCrypt Rehberi [59] bunu nasıl yapacağınızı açıklamaktadır.

Hassas bilgilerinizin teşhis edilme riskini göz önünde bulundurmamak

Çoğu zaman bilgisayarınızda ya da USB belleğinizde bir şifreleme [40] yazılımıyla 'yakalanmaktan' çok; şifrelenmiş bölümün, en çok korumak istediğiniz bilgileri tam nerede sakladığınıza işaret etmesinden endişe edersiniz. Her ne kadar bu bilgileri kimsenin okuyamayacağı gerçek olsa da bir saldırgan, onun orada olduğunu ve onu korumak için adımlar attığınızı bilecektir. Bu, saldırganın erişim elde etmek için girişebileceği, korkutma, şantaj, sorgulama ve işkence gibi çeşitli yöntemlere sizi açık hale getirebilir. İşte bu bağlamda, aşağıda ayrıntılarıyla betimlenen, TrueCrypt [58]'in inkâr edilebilirlik özelliği devreye girmektedir.

TrueCrypt [58]'in inkâr edilebilirlik özelliği, yazılımın, dosya şifreleme [40] araçlarının genel olarak sunduğunun ötesine geçtiği özelliklerden biridir. Bu özellik, en hassas bilgileri, diğerleri gibi yani daha az hassas, gizli veriler gibi gösteren steganografi [62]'nin nevi şahsına münhasır bir biçimi olarak düşünülebilir. Bu pek de gizli olmayan bir ofis kasasının içine 'gizli bir taban' kurmaya benzetilebilir. Saldırgan sizin anahtarınızı çalarsa ya da kasanın şifresini vermeniz için sizi korkutursa bulacağı şey korumayı gerçekten önemseydiğiniz bilgiler değil, bazı ikna edici 'yem' olarak kullandığınız materyaller olacaktır.

Kasanızın arkasında gizli bir bölme olduğunu sadece siz bileceksiniz. Bu, saldırganı vermiş olduğunuzdan başka bir sır sakladığınızı 'inkâr etmenizi' sağlayacaktır ve herhangi bir nedenden dolayı şifrenizi söylemek zorunda kaldığınızda bilgilerinizi korumanıza yardım edecektir. Bu nedenler, sizin ya da meslektaşınızın, tanıdıklarınızın, arkadaşlarınızın ve aile üyelerinizin güvenliği için hukukî ya da fiziksel tehditleri içerebilir. Inkâr edilebilirliğin amacı, verilerinizi korumayı seçerseniz bile potansiyel olarak tehlikeli bir durumdan kaçmanız için size bir şans vermektir. **Kendi kendinizi suçlu durumuna**

düşürme riskini göz önünde bulundurmak kısmında tartışıldığı gibi, ofisinizde bir kasayla yakalanmak kabul edilemez sonuçları beraberinde getirmek için yeterliyse, bu özellik daha az yararlıdır.

TrueCrypt ^[58]’in inkâr edilebilirlik özelliği, normal **şifrelenmiş** ^[40] bölümünüzün içine 'gizli bir bölüm' daha depolayarak işlev görür. Bu gizlenmiş bölümü, normal olarak kullandığınızdan farklı bir alternatif şifre kullanarak açarsınız. Teknik bilgiye sahip bir saldırgan standart bölümünüze erişse bile başka bir gizli bölümün olduğunu kanıtlayamayacaktır. Elbette **TrueCrypt** ^[58]’in bu yolla bilgi saklayabileceğini çok iyi bilebilir, bu nedenle yem olarak kullandığınız şifreyi verir vermez tehdidin ortadan kalkacağını garantisi yoktur. Çok sayıda insan **TrueCrypt** ^[58]’i, inkâr edilebilirlik özelliğine izin vermeden kullanmaktadır, bununla beraber verili bir **şifrelenmiş** ^[40] bölümün bu tür bir 'gizli tabanı'nın olup olmadığını, analiz yoluyla belirlemenin olanaksız olduğu düşünülmektedir. Buna rağmen, gizli bölümünüzü açık bırakmak ya da diğer uygulamaların onun içerdiği dosyalara kısayol oluşturmaya izin vermek gibi daha az teknik yollarla, gizli bölümünüzü açık etmediğinizden emin olmak sizin işinizdir. Alttaki **Okuma önerileri** ^[63] bölümü bu konu hakkında sizi daha fazla bilgiye götürebilir.

Claudia: Tamam, o zaman standart bölümün içine bazı işe yaramaz dosyaları koyalım ve tüm tanıklıkları da gizli olana taşıyalım. Eski PDF’lerin ya da kullanabileceğimiz başka şeylerin var mı?

Pablo: Ben de bunu düşünüyordum. Demek istediğim, başka seçeneğimiz yoksa yem olarak kullandığımız şifreyi vereceğiz, değil mi? Ama inandırıcı olmak için o dosyaların bir şekilde önemliymiş gibi görünmesini sağlamalıyız. Aksi halde onları neden şifreleyelim ki? Belki de ilgisiz malî dosyalar ya da web sitelerinin şifrelerinin bir listesini ya da bunun gibi bir şeyi kullanmalıyız.

Okuma önerileri

- Dosyalarınızı güvence altına almak için ek bilgi için, bakınız: [Digital Security and Privacy for Human Rights Defenders](#) ^[25] kitabının 2.4 *Cryptography*, 2.8 *Steganography* ve 4.2 *Case Study 3* bölümleri.
- [TrueCrypt Documentation](#) ^[64], bilgi şifrelemesinin birçok yönünü ayrıntılı bir şekilde ele almaktadır ve [TrueCrypt FAQ](#) ^[65] TrueCrypt hakkındaki bazı genel sorulara yanıt vermektedir.

5. Veri kayıpları nasıl kurtarılır

Dijital verilerin depolanmasının ya da transferinin her yeni yöntemi; söz konusu bilgilerin kaybedilmesinin, çalınmasının ya da tahrip edilmesinin birçok yeni yolunu beraberinde getirmeye eğilimlidir. Yılların emeği; hırsızlık, anlık dikkatsizlik, bilgisayar donanımlarına el konulması sonucunda ya da sadece dijital depolama teknolojisi doğası gereği kırılgan olduğundan bir anda ortadan kaybolabilir. Bilgisayar destekli çalışan profesyoneller arasında yaygın bir deyiş vardır: "Bu, verilerini *kaybedip kaybetmeyeceğin* sorunu değil; *ne zaman* kaybedeceğin sorundur." Öyle ise bu sizin başınıza geldiğinde, güncel bir yedeğe ve iyi test edilmiş geri yükleme araçlarına sahip olmanız çok önemlidir. Bir yedekleme sisteminin öneminin size hatırlatıldığı gün, genelde, bir yedekleme sisteminde sahip olmaya ihtiyaç duyduğunuz günün ertesi günüdür.

Etkili bir yedekleme politikası oluşturmak, her ne kadar güvenli bilgisayar kullanımının en temel unsuru olsa da görüldüğü kadar kolay değildir. Etkili bir yedekleme politikası oluşturmak, bir dizi nedenden dolayı planlama sırasında önünüze ilave engeller çıkarabilir: Özgün verileri ve yedekleri farklı fiziksel konumlara kaydetme gerekliliği, yedeklerin gizli tutulmasının önemi, her biri kendi taşınabilir depolama aygıtına sahip olan ve birbirleriyle bilgi paylaşan farklı insanlar arasında koordinasyonun güçlüğü... Yedekleme ve dosya kurtarma taktiklerine ek olarak, bu bölüm iki özgül araca işaret etmektedir, [Cobian Backup](#) ^[66] ve [Recuva](#) ^[67].

Arka plan senaryosu

Elena Rusça konuşulan bir ülkede, bölgedeki yasa dışı ağaç kesiminin hangi boyutlara ulaştığını göstermek için fotoğrafların, videoların, haritaların ve öykülerin sunumuna dayanan bir web sitesi oluşturmaya başlamış bir çevrecidir. Yıllardır ağaçların kesimi hakkında belgeler, medya dosyaları ve coğrafi bilgiler toplamaktadır ve bunların birçoğu çalıştığı STK’nin ofisindeki Windows işletim sistemli eski bir bilgisayarda depolanmaktadır. Bu bilgiler çevresinde bir web sitesi tasarlarlarken, bu bilgilerin korunmasının önemini fark etmeye başlar. Özellikle her şeyi web sitesine kopyalamadan önce bilgisayarının zarar görme ihtimali onu endişelendirir. Kurumunun diğer üyeleri de bu bilgisayarı zaman zaman kullanmaktadır. Çalışmasını içeren klasörü biri yanlışlıkla silerse bu klasörü nasıl kurtarabileceğini öğrenmek istemektedir. Yeğeni Nikolai’dan bir yedekleme stratejisi geliştirmek için yardım ister.

Bu bölümden ne öğrenebiliriz

- Bilgilerinizi nasıl düzenler ve yedeklersiniz
- Yedeklerinizi nerede muhafaza etmelisiniz
- Yedeklerinizi güvenli nasıl yönetebilirsiniz
- Yanlışlıkla silinen dosyaları nasıl kurtarırsınız

Bilgilerinizi tanımlamak ve düzenlemek

Felaketleri önlemek için verilerinizin fiziksel olarak güvende, **kötü amaçlı yazılımlardan** ^[2] arınmış, iyi bir **güvenlik duvarı** ^[68]

ve güçlü bir şifreyle korunuyor olduğundan emin olarak adım atmanız her ne kadar çok önemliyse de bu adımlar kendi başına yeterli değildir. Yanlış gidebilecek birçok şey vardır; virüs saldırıları, *hacker'lar* ^[1], elektrik kısa devreleri, ani voltaj yükselişleri, su dökülmeleri, çalınma, el konma, miknatıslanma, işletim sistemi çökmesi ve donanım hatası, bunlardan adını andığımız sadece birkaçıdır. Felaketlere hazırlanmak, ona karşı korunmak kadar önemlidir.

Elena: Yedeklemenin önemini biliyorum, Nikolai, fakat bu bir başkasının benim için bunu kurması gerektiği anlamına gelmiyor mu? Demek istediğim, bunu kendi başıma yapacak kadar zamana, kaynaklara ve deneyime sahip olacak mıyım?

Nikolai: Canını sıkma. İyi bir yedekleme planı yapmak biraz kafa patlatmayı gerektirir ama o kadar da çok zaman ve para gerektirmez. Bilgilerinin tümünü kaybetmekle kıyaslandığında bir yedekleme planı yapmanın külfetli olduğunu söyleyemezsin, değil mi? Dahası, yedekleme kesinlikle kendi başına yapman gereken şeylerden biridir. Hâlihazırda teknik destek vererek sana yardım eden kişiler son derece güvenilir ve dijital bilgilerini nerede sakladığını konusunda son derece bilgi sahibi değilse kendi başına bunu yapman daha iyidir.

Bir *yedekleme politikası* oluşturmanın ilk adımı, kişisel ve işle ilgili verilerinizin o anda nerede olduğunu gözünüzde canlandırmanızdır. Örneğin e-postanız internet servis sağlayıcınızın e-posta sunucusunda, bilgisayarınızda ya da her iki yerde birden depolanıyor olabilir. Ve elbette birden fazla e-posta hesabınız olabilir. O halde önemli belgeleriniz, iş yerinizde ya da evinizde kullandığınız bilgisayarınızdadır. Bilgisayarda adres defterleriniz, sohbet geçmişleriniz ve kişisel program ayarlarınız vardır. Bazı bilgilerinizin, USB bellekler, taşınabilir harici diskler, CD'ler, DVD'ler, ve eski disketler dahil çıkarılabilir araçlarda da depolanması olasıdır. Cep telefonunuzda bir kişiler listesi bulunur ve önemli yazılı mesajlar cep telefonunuzda depolanmış olabilir. Web siteniz varsa yılların emeği sonucu oluşmuş geniş bir makaleler koleksiyonu içerebilir. Ve son olarak, defterler, günlükler ve mektuplar gibi dijital olmayan bilgilerinizi unutmayın.

Ardından, bu dosyaların hangilerinin 'esas kopya' ve hangilerinin yedek kopya olduğunu belirlemeniz gerekir. Esas kopya, belirli bir dosyanın ya da dosyalar koleksiyonunun genellikle en güncel halidir ve içeriğini güncellenmeniz gerektiğinde gerçekten üzerinde çalıştığınız kopyaya karşılık gelir. Açıkta ki bu ayrım tek bir kopyası olan dosyalara uygulanamaz; ancak belirli türden bilgiler için aşırı derecede önemlidir. Yaygın bir felaket senaryosu, önemli bir belgenin sadece kopyaları yedeklendiğinde ve bu kopyaların güncellenmesinden önce, esas kopyanın kendisinin kaybolduğu ya da tahrip olduğu anda meydana gelir. Örneğin bir haftalığına seyahat ettiğinizi ve USB belleklerinizdeki belirli bir tablonun kopyasını güncellediğinizi hayal edin. Bu noktada, bu kopyanın sizin esas kopyanız olduğunu düşünmeye başlamalısınız çünkü ofisinizdeki güncel olmayan kopyanın düzenli ve otomatik alınan yedekleri artık işe yarar değildir.

Yukarıda tanımlanan bilginin tüm esas ve yedek kopyalarının fiziksel konumlarını yazmaya çalışın. Bu gereksinimlerinizi belirlemeye ve uygun bir yedekleme politikası tanımlamanıza yardım edecektir. Aşağıdaki tablo oldukça temel bir örnektir. Elbette listenizin çok daha uzun olduğunu ve birden fazla 'veri türünü' kapsayan bazı 'depolama aygıtlarını' içerdiğini ve bazı veri türlerinin de birden fazla aygıtta bulunduğunu fark edeceksiniz.

Veri Türü	Esas/Yedek	Depolama Aygıtı	Konum
Elektronik belgeler	Esas	Bilgisayar sürücüsü	İş
Birkaç önemli elektronik belge	Yedek	USB bellek	Yanımda
Program veri tabanları (fotoğraflar, adres defteri, ajanda, vb.)	Esas	Bilgisayar sürücüsü	İş
Birkaç önemli elektronik belge	Yedek	CD'ler	Ev
E-posta & e-posta kişileri	Esas	Gmail hesabı	İnternet
SMS'ler & cep telefonu kişiler listesi	Esas	Cep telefonu	Yanımda
Basılı belgeler (sözleşmeler, faturalar, vb.)	Esas	Çalışma masası çekmecesini	İş

Yukarıdaki tabloda görebileceğiniz gibi:

- Ofisinizdeki bilgisayarınızın sabit diski çöktüğünde belgelerinizden geriye kalacak olanlar sadece evinizdeki USB belleğinizdekiler ve CD kopyalarındaki yedeklerdir.
- E-posta mesajlarınızın ya da adres defterinizin çevrimdışı kopyasına sahip değilsiniz, öyle ki şifrenizi unuttuğunuzda (ya da biri kötü emellerle şifrenizi değiştirdiğinde) onlara erişiminizi yitireceksiniz.
- Cep telefonunuzdaki herhangi bir bilginin kopyasına sahip değilsiniz.
- Sözleşmeler ve faturalar gibi basılı belgelerin dijital ya da fiziksel kopyasına sahip değilsiniz.

Yedekleme stratejinizi tanımlamak

Yukarıdaki tüm veri türlerini yedeklemek için yazılımın ve atılması gereken bir dizi adımın bir kombinasyonuna gereksiniminiz olacak. Temelde, her bir veri türünün en az iki ayrı konumda depolandığından emin olmalısınız.

Elektronik belgeler - Aşağıda ayrıntılarıyla betimlenen *Cobian Backup* ^[66] gibi bir program kullanarak bilgisayarınızdaki belgelerin eksiksiz bir yedeğini oluşturun. Yedeği taşınabilir bir şeyde muhafaza edin ki evinize ya da bir başka güvenli yere onu götürebilesiniz. Harici sabit diskler, CD/DVD'ler ya da USB bellekler olası seçeneklerdir. Bazıları, üzerine yazma ya da yedeğini kaybetme riski daha düşük olduğundan bu iş için CD'leri ya da DVD'leri tercih etmektedir. Boş CD'ler her yedeklemede yeni bir tane kullanmanıza izin verecek kadar ucuz olabilir.

Bu veri kategorisi çoğu zaman en hassas bilgileri içerdiğinden elektronik belge yedeklerinizi şifreleme kullanarak yedeklemeniz özellikle önemlidir. Bunu nasıl yapacağınızı **4. Bölüm: Bilgisayarınızdaki hassas dosyaları nasıl**

korursunuz ^[41]'dan ve **TrueCrypt Rehberi** ^[59]'nden öğrenebilirsiniz.

Program veri tabanları - Program veri tabanlarınızın konumuna karar verdikten sonra, onları da elektronik belgelerle aynı şekilde yedekleyebilirsiniz.

E-posta - E-postalarınıza sadece bir web tarayıcısı aracılığıyla erişmek yerine, **Thunderbird** ^[69] gibi lokal bir e-posta programı kurun ve hesabınızla birlikte çalışacak şekilde onu düzenleyin. **Thunderbird Rehberi** ^[70] bunu nasıl yapacağınızı ayrıntılarıyla açıklar. Ayrıca birçok e-posta hizmeti de bu tür programları nasıl kullanacağınız ve çoğu zaman da e-posta adreslerinizi onlara nasıl aktaracağınız konusunda talimatlar sağlar. Bunun hakkında daha fazlasını Okumalar kısmında öğrenebilirsiniz. Eski e-posta mesajlarınızın (örneğin güvenlik gerekçeleriyle) sunucunuzda depolanmaması için bilgisayarınıza taşımaya karar verdiyseniz yukarıda betimlenen elektronik belgelerin yedeklenmesine onları da dahil ettiğinizden emin olun.

Cep telefonu içeriği - Cep telefonunuzdaki telefon numaralarını ve yazılı mesajları yedeklemek için telefonunuzu, genellikle telefonunuzun üreticisinin web sitesinde bulabileceğiniz uygun bir yazılım kullanarak bilgisayarınıza bağlayabilirsiniz. Bunun için özel bir USB kablo satın almanız gerekebilir.

Basılı belgeler - Mümkünse tüm önemli kağıtlarınızı taramalısınız, ardından da yukarıda ele alındığı gibi, diğer elektronik belgelerinizle birlikte yedeklemelisiniz.

Sonunda; depolama aygıtınızı, veri türlerinizi ve yedeklerinizi, bilgilerinizi felaketlere karşı daha dirençli kılacak şekilde yeniden düzenlemelisiniz:

Veri Türü	Esas/Yedek	Depolama Aygıtı	Konum
Elektronik belgeler	Esas	Bilgisayar sürücüsü	İş
Elektronik belgeler	Yedek	CD'ler	Ev
Birkaç önemli elektronik belge	Yedek	USB bellek	Yanımda
Veri Türü	Esas/Yedek	Depolama Aygıtı	Konum
Program veri tabanları	Esas	Bilgisayar sürücüsü	İş
Program veri tabanları	Yedek	CD'ler	Ev
Veri Türü	Esas/Yedek	Depolama Aygıtı	Konum
E-posta & e-posta kişileri	Yedek	Gmail hesabı	İnternet
E-posta & e-posta kişileri	Esas	İş yeri bilgisayarındaki Thunderbird	İş
Veri Türü	Esas/Yedek	Depolama Aygıtı	Konum
SMS'ler & cep telefonu kişiler listesi	Esas	Cep telefonu	Yanımda
SMS'ler & cep telefonu kişiler listesi	Yedek	Bilgisayar sürücüsü	İş
SMS'ler & cep telefonu kişiler listesi	Yedek	SIM kartında yedekli	Ev
Veri Türü	Esas/Yedek	Depolama Aygıtı	Konum
Basılı belgeler	Esas	Çalışma masası çekmecesini	İş
Taranmış belgeler	Yedek	CD'ler	Ev

Elena: Önemli belgelerini, taslaqlara ekleyerek ya da kendilerine e-posta göndererek Gmail'de saklayan insanlar tanyorum. Bu dosyalarım için 'ikinci fiziksel konum' olarak kabul edilebilir mi?

Nikolai: Bir ya da iki önemli belgeni kaybettiğinde onları kurtarmaya yardımcı olabilir ama oldukça garip bir yöntem. Doğruyu söylemek gerekirse bu şekilde bir haftada kaç belgeyi yedeklemek istersin? Dahası bu ekli belgelerin güvende olup olmadığını da göz önünde bulundurmalısın. Özellikle de e-postalarının izlendiği konusunda endişe ediyorsan... Gmail'e güvenli bir şekilde bağlanmıyorsan, bu, hassas bilgilerini gümüş bir tepside sunmaya benzer. Küçük Truecrypt dosyalarını ya da KeePass veri tabanı dosyalarını yedeklemek için Gmail'e bağlanmak için bir HTTPS kullanmak güvenli olabilir ama genel amaçlı yedekleme stratejisi olarak bunu kesinlikle tavsiye etmiyorum.

Dijital bir yedekleme yaratmak

Burada ele alınan veri tiplerinden bir yedekleme stratejisi oluştururken, insanların hakkında en çok endişe duydukları veri tipi 'elektronik belgeler'dir. Bu kavram her ne kadar muğlaksa da genellikle, kaydını kendinizin tuttuğu, ya çift tıklayarak ya da belirli bir uygulamanın dosya menüsünü kullanarak, manuel olarak açtığınız dosyaları işaret eder. Özellikle, diğer örneklerin yanı sıra metin dosyalarını, sözcük işlem belgelerini, sunumları, pdf'leri ve veri depolarını kapsar. Örneğin, e-posta mesajlarının aksine, elektronik belgeler internet üzerinden uzaktaki kopyalarıyla senkronize edilmezler.

Elektronik belgeleri yedeklerken program veritabanlarını da yedeklemeyi hatırlamalısınız. Örneğin bir takvim uygulaması ya da bir elektronik adres defteri kullanıyorsanız, bu programların verilerini depolamak için kullandığı klasörü de bulmanız gerekir. Umalım ki bu veritabanları elektronik belgelerinizle aynı konumda olsun, bunlar Windows tabanlı bilgisayarlarda genellikle *Belgelerim* klasörünün altında saklanır. Durum bu değilse, uygun klasörleri düzenli yedeklemenize eklemeniz

gerekir.

Thunderbird [69] gibi uygulamalar tarafından depolanan e-postalar bir programın veri tabanına özel bir örnektir. Bir e-posta programı kullanıyorsanız, özellikle de mesajınızın sunucuda bir kopyasını depolayamıyorsanız ya da depolamak istemiyorsanız, o halde e-posta veri tabanınızın düzenli yedeklemelerinize dahil olduğundan emin olmalısınız. Görüntü ve video dosyalarınızı, onlarla nasıl etkileşim halinde olduğunuza bağlı olarak, bir programın veri tabanındaki elektronik belgeler ya da nesneler olarak düşünebilirsiniz. Örneğin Windows Media Player ve iTunes gibi uygulamalar, veri tabanları gibi işler. Bu gibi programları kullanıyorsanız, yönetimine yardımcı oldukları gerçek medya dosyalarını nereye depoladıklarını öğrenmek için sabit diskinizi taramanız gerekebilir.

Depolama aygıtları

Elektronik belgelerinizi yedeklemeden önce, ne tür bir depolama aygıtı kullanacağınıza karar vermelisiniz.

USB bellekler - USB bellekler ucuz olabilir ve geniş kapasiteler sunabilir. Defalarca silmesi ya da üzerine yeniden yazması kolaydır. USB belleklerin, kullanım sıklığına ve biçimine bağlı olarak, sınırlı ömürleri vardır ama kullanım süreleri genellikle yaklaşık olarak 10 yıl olarak tahmin edilir.

Kompakt Diskler (CD'ler) CD'ler yaklaşık 700 Megabyte (MB) veri depolar. CD'lere yapılacak yedekleme için bir CD yazıcısına [71] ve boş disklere gereksiniminiz olacaktır. Bir CD'yi silmek ve kaydettiğiniz dosyaları yenilemek için bir CD-RW yazıcısına ve yeniden yazılabilir CD'lere gereksinimimiz olacaktır. Şimdilerde Windows XP dahil, belli başlı tüm işletim sistemleri, CD'ler ve CD-RW'ler yazabilen dahili bir yazılım içermektedir. Bu disklerle yazılan bilgilerin beş ya da on yıl sonra bozulmaya başlayabileceğini aklınızda bulundurmalısınız. Bu süreden daha uzun bir süre bir yedekleme depolamaya gereksinimimiz varsa bu CD'leri zaman zaman yeniden oluşturmanız, özel 'uzun ömürlü' diskler satın almanız ya da farklı bir yedekleme yöntemi kullanmanız gerekir.

Dijital Video Diskler (DVD'ler) - DVD'ler 4.7 Gigabyte'a (GB) kadar veri depolar. DVD'ler de CD'lere benzer şekilde çalışır ama biraz daha pahalı ekipmanlar gerektirir. Bir DVD ya da DVD-RW yazıcısına [71] uygun disklere gereksinimimiz olacaktır. Bir CD'de olduğu gibi normal DVD'ye yazılan veri, eninde sonunda silinmeye başlayacaktır.

Uzak sunucu - İyi düzenlenmiş bir ağ yedekleme sunucusu neredeyse sınırsız bir kapasiteye sahip olabilir ama internet bağlantınızın hızı ve istikrarı bunun gerçekçi bir seçenek olup olmayacağını belirleyecektir. Ofisinizde bir yedekleme sunucusu çalıştırmak her ne kadar internetten bilgi kopyalamaktan daha hızlı olsa da, önemli verilerinizin bir kopyasını iki farklı fiziksel konumda saklama gereksiniminizi ihlal eder. İnternette ücretsiz depolama hizmetleri bulunmaktadır ama bilgilerinizi çevrimiçi hale getirme riski üzerinde dikkatle düşünmelisiniz ve bilmediğiniz ya da güvenmediğiniz kuruluşlar ya da kişiler tarafından işletilen sunuculara yedeklemelerinizi yüklemekten önce onları daima şifrelemelisiniz. Birkaç örnek için Okuma önerileri [72] bölümüne bakınız.

Yedekleme Yazılımı

Cobian Yedekleme; düzenli olarak planlanmış zaman aralıklarıyla çalışması ve sadece son yedeklemeden sonra değiştirilen dosyaları içermesi için otomatik olarak ayarlanabilen, kullanıcı dostu bir araçtır. Ayrıca yedeklemeleri daha küçük hale getirmek için onları sıkıştırabilir.

Uygulama: Cobian Yedekleme Rehberi [73] ile uygulamaya başlayın

Her zaman olduğu gibi, yedekleme dosyalarınızı TrueCrypt [58] gibi bir araç kullanarak şifrelemek iyi bir fikirdir. Veri şifreleme konusunda daha fazla bilgi Bilgisayarınızdaki hassas dosyaları nasıl korursunuz [41] başlıklı **4. Bölüm** [41]'de bulunabilir.

Uygulama: TrueCrypt - Güvenli Dosya Depolama Rehberi [59] ile uygulamaya başlayın

Bu yedekleme araçlarını kullanırken yedekleme sisteminizin pürüzsüz bir şekilde işlemesine yardım etmek için yapabileceğiniz birkaç şey var:

- Bilgisayarınızdaki dosyaları düzenleyin. Yedeklemeye niyetlendiğiniz tüm elektronik belgeleri içeren klasörleri tek bir konuma, örneğin **Belgelerim** klasörüne taşımaya çalışın.
- Verilerini uygulama veri tabanında depolayan bir yazılım kullanıyorsanız öncelikle bu veri tabanının konumunu belirlemeniz gerekir. Bu uygun bir konum değilse programınızın veri tabanı için yeni bir konum seçmenize izin verip vermediğine bakın. İzin veriyorsa veri tabanını, elektronik belgelerinizle aynı klasöre yerleştirebilirsiniz.
- Yedeklemelerinizi gerçekleştirmek için düzenli bir zamanlama planı oluşturun.
- Ofisinizde güvenilir ve güvenli bir yedekleme politikası olmayan tüm çalışanlar için bir prosedür oluşturmaya çalışın. İş arkadaşlarınızın bu sorunun önemini anlamalarına yardımcı olun.
- Yedeklemenizden verilerinizi kurtarma işlemini test ettiğinizden emin olun. Nihayetinde sizin için gerçekten önemli olanın yedekleme prosedürü değil kurtarma prosedürü olduğunu aklınızda bulundurun!

Elena: Tamam, işteyken şifreli bir yedek oluşturdum ve onu bir CD'ye kaydettim. Cobian, yedeğimi birkaç gün içinde güncellemek üzere ayarlandı. İş yerindeki masamın kilitlenebilir bir çekmecesine var ve bu yedekleme CD'lerini, kaybolmasınlar ya da bozulmasınlar diye, orada saklamayı planlıyorum.

Nikolai: Ama ya iş yerin yanıp kül olursa? Diğer şeylerle birlikte, bilgisayar, masa, yedekleme CD'leri de...? Ya da web sitindeki forum büyük bir çevresel gösteri planlamaya karar verirse ve yetkililer müdahale eder ve işler çığırından çıkıp örgütüne baskın düzenlerlerse? Küçük masa kilidinin polislerin o CD'lere el koymasını engelleyebileceği konusunda

şüpheliyim. Yedeklerini evinde saklamaya ya da senin için saklaması için bir arkadaşına sormaya ne dersin?

Kazara silinen dosyaları kurtarmak

Windows'da bir dosyayı sildiğinizde, dosya ortalıktan kaybolur ama içeriği bilgisayarda kalır. **Geri Dönüşüm Kutusu**'nu boşalttıktan sonra bile, sildiğiniz dosyadaki bilgiler genelde hala sürücünüzde bulunabilir. Bu konuda daha fazla şey öğrenmek için **Hassas bilgiler nasıl imha edilir** ^[61] başlıklı **6. Bölüm** ^[61]'e bakınız. Zaman zaman önemli bir dosyanızı ya da klasörünüzü kazara silerseniz, bu güvenlik açığı sizin lehinize işleyebilir. Kısa süre önce silinmiş dosyalara erişimi yeniden sağlayabilecek, **Recuva** ^[74] adlı bir araç dahil, birçok program vardır.

Uygulama: **Recuva - Dosya Kurtarma Rehberi** ^[74] ile uygulamaya başlayın

Bu araçlar her zaman çalışmaz çünkü Windows, silinmiş bilgilerin üzerine yeni veriler yazmış olabilir. Bu nedenle bir dosyayı silmeniz ve **Recuva** ^[74] gibi bir araçla onu kurtarmaya girişmeniz arasında geçen sürede bilgisayarınızla olabildiğince az şey yapmanız önemlidir. Dosyayı kurtarma işine girişmeden önce bilgisayarınızı ne kadar uzun süre kullanırsanız, başarılı olma şansınız o kadar azalır. Bu, aynı zamanda, önemli bir dosyayı sildikten sonra **Recuva**'yı kurmak yerine **Recuva**'nın taşınabilir bir versiyonunu kullanmanız gerektiği anlamına gelir. Bir yazılımı kurmak dosya sistemine yeni bilgiler yazmayı gerektirir ki bu bilgiler, kurtarmaya çalıştığınız önemli verinin üzerine rastlantısal olarak yazılabilir.

Bu bölümde betimlenen politikaları uygulamak ve araçları öğrenmek her ne kadar büyük bir işmiş gibi görünse de bir kez oturmuş bir sisteme sahip olduğunuzda, yedekleme stratejinizi sürdürmek, ilk seferine göre çok daha kolay hale gelecektir. Ve yedekleme, veri güvenliğinin en önemli boyutu olduğundan, bu süreci geçmiş olmanızın çabalarınıza değdiğinden emin olabilirsiniz.

Okuma önerileri

- Yedekleme ve veri kurtarma hakkında daha fazla bilgi **Digital Security and Privacy for Human Rights Defenders** ^[25] kitabının 2.3 *Information Backup, Destruction and Recovery* bölümünde bulunabilir.
- Çevrimiçi yedeklemenin yeni riskleri beraberinde getireceğini göz önünde bulundurun. En azından sunucuya yüklemekten önce **hassas bilgilerinizi ayrıca kendiniz şifrelemeyi hatırlayınız**. Yukarıda belirtilen adımı attığınızı varsayarak, bilgilerinizi yedeklemenin uygun bir yolu olarak ücretsiz veri depolama hizmetleri bulunmaktadır. Bunlardan bazıları: **Wuala** ^[75], **SpiderOak** ^[76], **Google Drive** ^[77], **tahoe-lafs** ^[78].
- Veri kurtarma üzerine **Wikipedia** ^[79]'da mükemmel bir makale bulunmaktadır.

6. Hassas bilgiler nasıl imha edilir

Önceki bölümler hassas bilgilerinizi korumanıza yardım edebilecek bir dizi aracı ve alışkanlığı ele aldı; ancak bir bilgiyi saklamanız gerekmediğine karar verdiğinizde ne olur? Örneğin belirli bir dosyanın şifrelenmiş yedek kopyalarının yeterli olduğuna karar verdiğinizde ve esas kopyayı silmek istediğinizde bunu yapmanın en iyi yolu nedir? Ne yazık ki, yanıt sandığınızdan daha karmaşık olabilir. Bir dosyayı sildiğinizde, **Geri Dönüşüm Kutusu**'nu boşalttıktan sonra bile, belgenin içeriği sabit diskinizde kalır ve uygun araçlara ve biraz da şansa sahip olan herhangi biri tarafından kurtarılabilir.

Silinmiş bilgilerin yanlış ellere geçmemesini güvence altına almak için verileri güvenli ve kalıcı olarak ortadan kaldıran özel yazılımlar kullanmanız gerekir. **Eraser** ^[80] aşağıda ele alınan bu araçlardan biridir. **Eraser** ^[80]'ı kullanmak, kağıt belgeleri kimsenin bulmayacağını umut ederek basitçe çöp sepetine atmak yerine onları küçük parçalara ayırmaya benzer. Ve elbette dosyaları silmek, hassas bilgileri ortadan kaldırmanızı gerektiren durumların sadece bir örneğidir.. Birinin, özellikle güçlü ve siyasi olarak motive olmuş bir rakibinizin, sildiğinizi düşündüğünüz belirli dosyaları okuyarak siz ve kuruluşunuz hakkında bir şeyler öğrenebileceğinin ayrıntılarını göz önünde bulundurduğunuzda, muhtemelen kalıcı olarak silmek isteyebileceğiniz başka veri örnekleri de aklınıza gelecektir. Örneğin, günü geçmiş yedeklemeleri imha etmek, elden çıkarmadan önce eski sabit disklerinize **kalıcı silme işlemi** ^[81] uygulamak, internet tarayıcınızın geçmişini temizlemek... **CCleaner** ^[82], bu bölümde ele alınan ve işletim sisteminizin ve uygulamalarınızın her kullandığınızda oluşturduğu geçici dosyaları silerken karşılaşılabilecek zorluklar konusunda size yardımcı olabilecek bir başka araçtır.

Arka plan senaryosu

Elena, Rusça konuşulan bir ülkede, bölgedeki yasa dışı ağaç kesiminin hangi boyutlara ulaştığını göstermek için fotoğrafların, videoların, haritaların ve öykülerin sunumuna dayanan bir web sitesi oluşturmaya başlamış bir çevrecidir. Web sitesini yaparken kullandığı bilgilerin bir yedeğini oluşturmuştur ve kopyalarını evinde, iş yerinde ve yeni dizüstü bilgisayarında saklamaktadır. Kısa bir süre önce web sunucusunun ziyaretçi kayıtlarını ve kullanıcıların forum gönderilerini içeren veritabanının da bir kopyasını depolamaya başlamıştır. Elena yakın zamanda çevreci aktivistlerin uluslararası bir konferansına katılmak için yurt dışına seyahat edecektir. Sınırı geçerken aktivistlerden bazılarının dizüstü bilgisayarlarına bir saati aşkın bir süreliğine el konulduğu haberi verilmişti. Hassas bilgilerini ve daha siyasi olan forum katılımcılarının güvenliğini korumak için, evindeki ve iş yerindeki yedekleri bir TrueCrypt bölümüne taşıdı ve dizüstü bilgisayarındaki kopyayı da sildi. Tavsiyede bulunması için yeğeni Nikolai'e danıştı ve o da, sınır görevlileri tarafından bilgisayarına el konulmasından endişe ediyorsa eski yedeklerini sadece silmekten daha fazlasını yapması gerektiği konusunda onu uyardı.

Bu bölümden ne öğrenebilirsiniz

- Hassas bilgilerinizi bilgisayarınızdan kalıcı olarak nasıl silebilirsiniz
- CD'ler ve USB bellekler gibi taşınabilir depolama aygıtlarındaki bilgilerinizi nasıl ortadan kaldırabilirsiniz
- Bilgisayarınızda yakın zamanda hangi belgelere göz attığınızı başkalarının öğrenmesini nasıl önlersiniz
- Silinmiş dosyalarınız gelecekte kurtarılamayacak şekilde bilgisayarınızı nasıl muhafaza edersiniz

Bilgileri silmek

Tamamen teknik bir perspektiften bakacak olursak, bilgisayarınızda silme işlevi diye bir şey yoktur. Elbette bir dosyanızı Çöp Kutusu'na taşıyabilirsiniz ve Çöp Kutusu'nu boşaltabilirsiniz ancak bütün bunların gerçekte yaptığı şey, dosyanın ikonunu temizlemek, bilgisayarınızdaki her şeyin gizlenmiş dizininden dosyanın adını kaldırmak ve Windows'a bu alanı başka bir şey için kullanabileceğini söylemektir. Windows, bu alanı gerçekten kullanıncaya kadar, bu alan, silinen bilginin içeriği tarafından işgal edilmeye devam edecektir. Tıpkı tüm etiketleri kaldırıldığı halde özgün dosyaları barındırmaya devam eden bir dosya dolabı gibi. Bu nedenle, doğru yazılıma sahipseniz ve yeterince hızlı hareket ederseniz **Veri kayıpları nasıl kurtarılır** ^[43] başlıklı **5. Bölüm** ^[43]'de ele alındığı gibi kazara sildiğiniz bilgileri geri getirebilirsiniz.

Ayrıca bilgisayarınızı her kullandığınızda, sizin bilginiz olmaksızın, dosyaların oluşturulduğunu ve güvenli olmayan bir biçimde silindiğini aklınızda bulundurmalısınız. Örneğin kapsamlı bir rapor yazdığınızı varsayın. Bir haftadır her gün birkaç saat çalışarak bu rapor üzerine çalıştınız; belgenizi kaydettiğiniz her seferinde Windows, belgenin yeni bir kopyasını oluşturacak ve sabit diskinizde depolayacaktır. Belgenizin birkaç gün süren düzenlemelerinden sonra, hepsi farklı tamamlanma aşamalarında olan birçok versiyonunu, farkında olmaksızın kaydetmiş olabilirsiniz.

Genellikle Windows bir dosyanın eski versiyonlarını siler, elbette, ama yeni bir kopya meydana getirildiğinde güvenli olarak üzerine yazmak için özgün olanın tam yerine bakmaz. Bunun yerine basitçe, yukarıda sözü geçen metaforik dosya dolabının yeni bir bölümüne son versiyonu yerleştirir, eski bölümün etiketini yenisine taşır ve başka bir program, alana gereksinim duyuncaya kadar da eski taslağı olduğu yerde bırakır. Açık ki dosya dolabınızdan belgenin tüm izlerini imha etmek için iyi bir nedeniniz varsa, son kopyayı ortadan kaldırmak yeterli olmayacaktır ve sadece etiketi söküp atmak daha da kötü sonuç verecektir.

Bilgisayar sabit disklerinin dijital bilgi depolayan tek aygıt olmadığını da hatırlayın. CD'ler, DVD'ler, USB bellekler, disketler, cep telefonlarının hafıza kartları ve taşınabilir harici diskler de aynı sorunlara sahiptir ve bunlardan hassas bilgilerin temizlenmesinde basit bir silme ve yeniden yazma işlemine güvenmemeniz gerekir.

Güvenli silme araçlarıyla bilgileri kalıcı olarak silmek

Bu bölümde tavsiye edilenler gibi güvenli bir silme aracı kullandığınızda, hassas bilgilerinizi basitçe silmek yerine bu bilgileri bir başkasıyla değiştirdiğinizi ya da bu bilgilerin 'üzerine yazmış' olduğunuzu söylemek daha doğru olacaktır. Yukarıda varsayılan dosya dolabında saklanan belgelerin kurşun kalemle yazılmış olduğunu hayal edecek olursanız, güvenli silme yazılımı sadece içeriği silmekle kalmaz ayrıca her sözcüğün üzerini de karalar. Ve kurşun kalem izi gibi, dijital bilgiler de silinseler ve üzerlerine başka bir şey yazılsa bile, her ne kadar az da olsa, okunabilir. Bu nedenle burada tavsiye edilen araçlar gelişigüzel seçilen verilerle dosyaların üzerine defalarca yazar. Bu işlem, **kalıcı silme işlemi** ^[81] (**wiping** ^[81]) olarak adlandırılır ve bilginin üzerine ne kadar çok yazılırsa birinin özgün içeriği kurtarması da o kadar güçleşir. Uzmanlar genellikle üç ve daha fazla yazma işleminin yapılması gerektiği konusunda hemfikir; bazı standartlar ise yedi ve daha fazlasını gerektirir. **Kalıcı silme** ^[81] yazılımı, otomatik olarak bilginin üzerine makul bir sayıda yazma işlemi yapar ama istediğiniz takdirde bu sayıyı değiştirebilirsiniz.

Dosyaları kalıcı olarak silmek

Sabit diskinizden ya da depolama aygıtınızdan hassas verilerinize **kalıcı silme işlemi** ^[81] uygulamanın iki genel yolu vardır. Tek bir dosyaya ya da diskteki 'atanmamış' alanın tamamına **kalıcı silme işlemi** ^[81] uygulayabilirsiniz. Bu kararı verirken daha önce önerilen diğer varsayımsal örnekleri (uzun raporunuz hazırlanırken her ne kadar sadece bir dosya görünür halde olsa da dosyanın birçok tamamlanmamış kopyasının sabit diskinizin çeşitli yerlerine bırakılmış olabileceği gibi) düşünmeniz yararlı olur. Dosyanın kendisine **kalıcı silme işlemi** ^[81] uygularsanız, son sürümünü ortadan kaldırdığınızdan emin olabilirsiniz ama diğer kopyaları oldukları yerde bırakmış olursunuz. Aslında bu kopyaları doğrudan hedef almanın bir yolu yoktur çünkü özel bir program kullanılmadığı sürece görünür değildir. Bununla beraber depolama aygıtınızdaki tüm boş alana **kalıcı silme işlemi** ^[81] uygulayarak tüm önceden silinmiş bilgilerin yok edilmesini güvence altına alırsınız. Kötü etiketlenmiş dosya dolabı metaforuna dönersek, bu işlem dolabın tamamını aramaktan ziyade etiketleri çoktan çıkarılmış herhangi bir belgenin üzerini tekrar tekrar silmek ve yeniden yazmakla karşılaştırılabilir.

Eraser ^[80] ücretsiz, kullanması oldukça kolay açık kaynak kodlu bir güvenli silme aracıdır. **Eraser** ^[80] ile dosyalara üç farklı şekilde **kalıcı silme işlemi** ^[81] uygulayabilirsiniz: bir dosyayı seçerek, Geri Dönüşüm Kutusu'nun içeriğini seçerek ya da diskteki 'atanmamış' alanın tamamına **kalıcı silme işlemi** ^[81] uygulayarak. **Eraser** ^[80] ayrıca aşağıda ele alınan Windows'un **swap dosyalarının** ^[83] içeriğine de **kalıcı silme işlemi** ^[81] uygulayabilir.

Uygulama: **Eraser - Güvenli Dosya Kaldırma Rehberi** ^[84] ile uygulamaya başlayın

Güvenli silme araçları, görünür dosyalarınıza özel olarak **kalıcı silme işlemi** ^[81] uygulamadığınız sürece bu dosyalara zarar vermez; ancak yine de bu tür yazılımları kullanırken tedbirli olmak önemlidir. Her şeye rağmen kazalar olabilmektedir; insanların **Geri Dönüşüm Kutularını** ve veri kurtarma araçlarını faydalı bulmalarının nedeni de budur. Bir şeyleri sildiğiniz her seferinde verilerinize **kalıcı silme işlemi** ^[81] uygulamayı alışkanlık haline getirdiyseniz kendinizi basit bir hatadan kurtaramaz durumda bulabilirsiniz. Bilgisayarınızdan büyük miktarda veriye **kalıcı silme işlemi** ^[81] uygulamadan önce

güvenli bir yedeklemeye sahip olduğunuzdan daima emin olun.

Elena: Microsoft Word ve Open Office gibi kelime işlemci programların, üzerinde çalıştığınız dosyanın zaman zaman geçici kopyalarını oluşturduğunu biliyorum. Diğer programlar da bunu yapıyor mu ya da sadece kendi oluşturduğum ve sildiğim dosyalar için mi endişelenmeliyim?

Nikolai: Aslında programların kişisel verilerinin ve çevrimiçi etkinliklerinin izlerini bilgisayarında bıraktıkları birçok yer vardır. Ziyaret ettiğin web sitelerinden, kısa bir süre önce üzerinde çalıştığın taslak e-postalarından ve buna benzer şeylerden söz ediyorum. Tüm bunlar o bilgisayarı hangi sıklıkla kullandığına bağlı olarak hassas bilgiler olabilir.

Geçici verileri kalıcı olarak silmek

Eraser [80]'ın sabit diskinizdeki tüm atanmamış alana kalıcı silme işlemi [81] uygulamanıza izin veren özelliği görüldüğü kadar riskli değildir çünkü Eraser [80] sadece daha önceden silinmiş içeriği kalıcı olarak siler [81]. Normal, görünür dosyalar etkilenmeyecektir. Diğer yandan bu olgu ayrı bir sorunu aydınlatmaya hizmet eder: Eraser [80] silinmemiş ama oldukça iyi gizlenmiş hassas bilgilerinizin temizlenmesine yardım edemeyecektir. Bu tür verileri içeren dosyalar, muğlak klasörlere tıklanmış olabilir ya da anlamsız dosya adlarıyla depolanmış olabilir. Bu, elektronik belgeler için önemli bir sorun değildir ama bilgisayarınızı her kullandığınızda otomatik olarak biriken bilgiler için oldukça önemli olabilir. Örnekler şunlardır:

- Web sayfalarını gösterirken tarayıcınız tarafından kaydedilen metinleri, resimleri, çerezleri [85] (cookies [85]), hesap bilgilerinizi, çevrimiçi formları tamamlamak için kullanılan kişisel verileri ve ziyaret ettiğiniz sitelerden oluşan geçmiş de içeren geçici veriler.
- Yaptığınız işi kaydetmeden bilgisayarınızın çökmesi durumunda işlerinizi kurtarmanıza yardım etmek için çeşitli uygulamalar tarafından kaydedilen geçici dosyalar. Bu dosyalar diğer potansiyel olarak hassas bilgilerin yanı sıra metinleri, resimleri, tablo verilerini ve diğer dosyaların adlarını içerebilir.
- Kolaylık adına Windows tarafından saklanan dosyalar ve bağlantılar; örneğin, yakın zamanda kullandığınız uygulamalara kısayollar, gizli kalmasını tercih edebileceğiniz klasör bağlantıları ve elbette boşaltmayı unuttuğunuz Geri Dönüşüm Kutusu'nun içeriği.
- Windows swap dosyası [83]. Bilgisayarınızın hafızası dolduğunda, örneğin eski bir bilgisayarda aynı anda birçok programı çalıştırdığınızda olduğu gibi, Windows verilerinizi swap dosyası [83] adı verilen tek bir geniş dosyaya zaman zaman kopyalar. Sonuç olarak bu dosya, web sayfaları, dosya içerikleri, şifreler ve şifrelenmiş dosyalar dahil, hemen hemen her şeyi içerebilir. Bilgisayarınızı kapattığınız zaman bile swap dosyası [83] ortadan kaldırılmaz, bu nedenle onu siz silmelisiniz.

Sıkça rastlanan geçici dosyaları bilgisayarınızdan silmek için CCleaner olarak adlandırılan ücretsiz bir aracı kullanabilirsiniz. CCleaner [82], her biri potansiyel olarak hassas bilgileri açığa çıkardığı bilinen Internet Explorer, Mozilla Firefox [13] ve Microsoft Office uygulamaları gibi yazılımların kullanımı sonrasında bilgisayarınızın temizlenmesi için tasarlanmıştır. Bu araç ayrıca Windows'un kendisini de temizler. CCleaner [82] her çalıştırılmadan sonra dosyalarınızı güvenli silme becerisine sahiptir. Böylece, sabit diskinizdeki atanmamış alana Eraser [80] kullanarak kalıcı silme işlemi [81] uygulamak zorunluluğundan sizi kurtarır.

Uygulama: CCleaner - Güvenli Dosya Silimi ve Bilgisayar Kullanım Geçmişinin Kalıcı Olarak Silinmesi Rehberi [86] ile uygulamaya başlayın

Güvenli silme araçlarını etkin bir şekilde kullanmak için ipuçları

Her ne kadar hassas dosyaları silmek konusunda dikkatli olsanız da bilgilerinizin bilgisayarınızda ya da depolama aygıtınızda görünebilir kılındığı bir kaç yoldan artık haberdarsınız. Bu bilgileri kalıcı olarak silmek [81] için hangi araçları kullanabileceğinizi de biliyorsunuz. Diskinizin güvenli ve etkin bir şekilde temizlenmesini güvence altına almak için, özellikle bu tür araçları ilk defa kullanıyorsanız, izlemeniz gereken birkaç basit adım vardır:

- Veri kayıpları nasıl kurtarılır [43] başlıklı **5. Bölüm** [43]'de ele alındığı gibi, önemli dosyalarınızın şifrelenmiş bir kopyasını oluşturun.
- Gerekli olmayan tüm programları kapatın ve internet bağlantınızı kesin.
- Tüm depolama aygıtlarınızdan gereksiz dosyalarınızı silin ve **Geri Dönüşüm Kutusu**'nu boşaltın.
- Geçici dosyalarınızı CCleaner [82] kullanarak kalıcı olarak silin [81].
- Windows swap dosyasını [83] Eraser [80] kullanarak kalıcı olarak silin [81]
- Bilgisayarınızdaki ve diğer depolama aygıtlarınızdaki boş alanı Eraser [80] kullanarak kalıcı olarak silin [81]. Bu işlem oldukça yavaş olabileceğinden, bilgisayarınızı gece boyunca çalıştırmanız gerekebilir.

Bundan böyle şunları alışkanlık haline getirmeniz gerekir:

- Geçici dosyaları düzenli olarak CCleaner [82] kullanarak kalıcı olarak silmek [81].
- Hassas elektronik belgelerinizi, **Geri Dönüşüm Kutusu**'nu ya da Windows'un silme işlevini kullanarak silmek yerine Eraser [80] kullanarak kalıcı olarak silmek [81].
- Windows swap dosyasını [83] belirli aralıklarla Eraser [80] kullanarak kalıcı olarak silmek.
- Yakın zamanda içerdiği hassas bilgilerin silinmiş olabileceği sabit diskinizdeki, USB belleklerinizdeki ve diğer depolama aygıtlarınızdaki atanmamış alanı Eraser [80] kullanarak silin. Bu işlem oldukça yavaş olabileceğinden bilgisayarınızı gece boyunca çalıştırmanız gerekebilir. Bunlar disketleri, yeniden yazılabilir CD'leri, DVD'leri ve kameraların, cep telefonlarının ya da taşınabilir müzik çalarların hafıza kartlarını içerebilir.

Bir depolama aygıtının tüm içeriğini kalıcı olarak silmek üzerine ipuçları

Bir depolama aygıtının tamamına, zaman zaman [kalıcı silme işlemi](#) ^[81] uygulamanız gerekebilir. Eski bir bilgisayarınızı satacağınız ya da elden çıkaracağınız zaman bilgisayarın sabit diskini çıkarmanız; bilgisayarın yeni sahibinin de yeni bir sabit disk edinmesi en iyisidir. Bu mümkün değilse sabit disk vermeden önce, onu en azından [Eraser](#) ^[80]'la en ince ayrıntısına kadar [kalıcı olarak silmeniz](#) ^[81] gerekir. Sürücüyü elinizde bulunduracaksanız, ister yeniden kullanın isterseniz devre dışı bırakın, her hâlükârda sabit diskinize [kalıcı silme işlemi](#) ^[81] uygulamak isteyebilirsiniz. Benzer bir şekilde, yeni bir disk sürücüsü satın aldığınızda eski sürücünüzdeki verileri kopyaladıktan ve güvenli bir yedekleme oluşturduktan sonra, eski sürücünüze [kalıcı silme işlemi](#) ^[81] uygulamalısınız. Eski sürücünüzü atmaya ya da geri dönüştürmeye niyetliyseniz onu fiziksel olarak tahrip etmeyi de düşünmelisiniz. (Birçok bilişim danışmanı, önceden hassas bilgiler içeren herhangi bir veri depolama aygıtının kullanımdan çıkarılmasından önce çekiçle birkaç güçlü darbe vurulmasını tavsiye eder).

Yukarıda betimlenen herhangi bir durumda, sürücünüzün tamamına [Eraser](#) ^[80] kullanarak [kalıcı silme işlemi](#) ^[81] uygulamanız gerekir ki bu işlem, bilgisayarınızın işletim sistemi bahsi geçen sürücüde çalışıyor olduğu sürece imkansızdır. Bu sorunu aşmanın en kolay yolu sürücüyü sökmeniz ve onu harici USB "sürücü kutusu"na koyarak, [Eraser](#) ^[80]'ın kurulu olduğu herhangi bir bilgisayara bağlamanızdır. Bu durumda harici sürücünüzün tüm içeriğini silebilirsiniz ve [Eraser](#) ^[80]'la onun tüm atanmamış alanına [kalıcı silme işlemi](#) ^[81] uygulayabilirsiniz. Bu işlem oldukça zaman alır, neyse ki sık sık yapmanız gereken bir şey değildir.

Yeniden yazılabilir CD'de ya da DVD'de depolanan verilere [kalıcı silme işlemi](#) ^[81] uygulamaya çalışmak yerine çoğu zaman onları tahrip etmek daha iyidir. Gerekliyse saklamak istediğiniz bilgilerle yeni bir disk oluşturabilirsiniz. Ve elbette yeniden yazılabilir olmayan diskler için bu, 'silme'nin tek yoludur. CD'nin ya da DVD'nin içeriğini tamamen tahrip etmek şaşırtıcı bir şekilde güçtür. Küçük parçalara ayrılmış dahi olsalar bu tür disklerden bilgilerin kurtarıldığına ilişkin öyküleri duymuş olabilirsiniz. Her ne kadar bu öyküler doğruysa da bu bilgileri bu yolla yeniden inşa etmek uzun zaman ve uzmanlık gerektirir. Birilerinin bilgilerinize erişmek için böyle bir çabayı gösterip göstermeyeceğine kendiniz karar vermelisiniz. Güçlü bir makas (ya da çok güçlü bir kağıt imha makinesi) için üstesinden gelecektir. Ek önlemler almak istiyorsanız ortaya çıkan parçaları evinizden ya da iş yerinizden uzaktaki çeşitli yerlere atabilirsiniz.

Elena: İnternet sunucu kayıtlarının eski CD yedekleri hala elimde ve CD'lerin mikro dalga fırınlara konarak silinebileceğini duydum. Yine de bir şekilde bu bana kötü bir fikir gibi göründü. İnsanlar gerçekten bunu yapıyor mu? İşe yarıyor mu?

Nikolai: Verileri oldukça etkili bir şekilde imha ettiğini düşünüyorum ama bir CD'yi mikro dalga fırına hiç koymadığım için bilmiyorum. Haklısın. Kötü bir fikir gibi görünüyor. Diyelim ki metaller mikro dalga fırınına zarar vermedi ya da yangın çıkarmadı; plastiğin hiç de sağlıklı olmayan dumanlar çıkaracağına iddiaya varım. Üzerinde düşünecek olursak, CD'lerini bir ateşte yakmanı da tavsiye etmem.

Okuma önerileri

- Her ne kadar Firefox, kendi geçici dosyalarını kalıcı bir şekilde silmek için güvenli silme teknikleri kullanmasa da, bu dosyaların çoğunu temizlemek için yerleşik bir araç temin etmektedir. Bu özellik [Firefox Rehberi](#) ^[14]'nde anlatılmaktadır.
- Ccleaner'in kurulması ve kullanımıyla ilgili ilave bilgi için bakınız: [CCleaner FAQ](#) ^[87]
- Her ne kadar metnin çoğu oldukça teknik olsa da, Peter Gutmann'ın [Secure Deletion of Data from Magnetic and Solid-State Memory](#) ^[88] yazısının giriş bölümü okumaya değer. Öyle ki bu metinde anlatılan [metodun](#) ^[89] [Eraser](#) ve diğer dosya silme araçları geliştiricilerinin üzerinde büyük bir etkisi olmuştur.

7. İnternet iletişiminizin gizliliği nasıl korunur

E-postanın ve anlık mesajlaşmanın kullanım kolaylığı, düşük maliyeti ve esnekliği internete en sınırlı erişimi olan kişiler ve kuruluşlar için bile bunları aşırı değerli kıldı. Daha hızlı ve güvenli bağlantıları olanlar için [Jitsi](#) ^[90], [Skype](#) ^[34] ve diğer [IP Üzerinden Ses VoIP](#) ^[91] araçları gibi yazılımlar da bu özellikleri paylaşır. Ne yazık ki geleneksel iletişim araçlarına alternatif olarak gelen bu dijital araçlara hassas bilgilerin gizliliğini korumak hususunda her zaman güvenilemez. Postayla gönderilen mektuplar, telefonla yapılan aramalar ve yazılı mesajlar da saldırıya açıktır; özellikle yetkililerin takibinin hedefi olanlar tarafından kullanıldığında.

Dijital, internet-tabanlı iletişim teknikleriyle daha geleneksel yöntemler arasındaki bir önemli farklılık, ilkinin kendi güvenlik düzeyinizi belirlemenize çoğu zaman izin vermesidir. Güvenli olmayan yöntemlerle e-postalar, anlık mesajlar ve [VoIP](#) ^[91] gönderileri göndermek, mektuplardan ve telefon görüşmelerinden neredeyse kesinlikle daha az gizlidir. Kısım bu, birkaç güçlü bilgisayarın büyük miktardaki dijital bilgi içinden göndericileri, alıcıları ve belirli anahtar sözcükleri tespit etmek için otomatik olarak tarayabilesindendir. Geleneksel iletişim kanalları üzerinden aynı düzeyde bir takibi gerçekleştirmek için çok daha büyük kaynaklar gerekir. Bununla beraber belirli önlemleri alırsanız tersi de doğrudur. İnternet iletişim araçlarının esnekliği ve modern [şifrelemenin](#) ^[40] gücü, sadece ulusal ordu ve istihbarat örgütleri için mümkün olan bir gizlilik düzeyini günümüzde sağlayabilir.

Burada verilen tavsiyeleri izleyerek ve bu bölümde ele alınan yazılımları inceleyerek iletişim güvenliğinizi büyük oranda artırabilirsiniz. [RiseUp](#) ^[92] e-posta hizmeti, [Pidgin](#) ^[93] anlık mesajlaşma programı için Off the Record [OTR](#) ^[94] (Kayıt Dışı)

eklentisi, Mozilla [Firefox](#) [13] ve Mozilla [Thunderbird](#) [69] e-posta sunucusu için [Enigmail](#) [95] eklentilerinin hepsi mükemmel araçlardır. Bununla beraber bunları kullanırken verili bir haberleşmenin gizliliğinin hiçbir zaman yüzde yüz garanti edilemeyeceğini aklınızda bulundurmalısınız. Her zaman göz önünde bulundurmadığınız bazı tehditler bulunur; diyelim bilgisayarınızda bir [keylogger](#) [96] bulunması, kapınızı dinleyen biri, dikkatsiz bir e-posta alıcısı ya da tamamen farklı bir olasılık... Bu bölümün amacı, aklınıza gelmeyen tehditleri bile azaltmak için size yardımcı olmaktır. Ancak bu bölümde bunu yaparken, bazılarının tercih ettiği 'kamuya açık etmek istemediğin hiçbir bilgiyi internetten göndermemelisin' seçeneğinden kaçınacağız.

Claudia ve Pablo, Güney Afrika ülkelerinden birindeki bir insan hakları STK'siyle birlikte çalışmaktadır. Bölgede ordu tarafından işlenen insan hakları ihlalleri konusunda aylar boyunca tanıklıklar topladıktan sonra Claudia ve Pablo elde ettikleri verileri korumak için adımlar atmaya başlamıştır. Sadece ihtiyaçları olan bilgiyi ellerinde tuttular ve bu bilgiyi, birçok fiziksel konumda yedeklenmiş bir TrueCrypt bölmesinde depoladılar. Bir raporda bu tanıklıkların belirli bölümlerini yayınlamaya hazırlanırken bir başka ülkedeki meslektaşlarıyla hassas bilgileri tartışmaları gerektiğini fark ettiler. Her ne kadar adları ve konumları belirtmemek konusunda hemfikirlerse de bu konu üzerinde yapılacak olan e-posta ve anlık mesajlaşma iletişimlerinin güvenli olmasından emin olmak istemektedirler. Claudia iletişim güvenliğinin önemini ele almak amacıyla bir toplantı için çağrı yaptıktan sonra ofistekilerin bir sorusu olup olmadığını sordu.

Bu bölümden ne öğrenebilirsiniz

- Birçok webmail ve anlık mesajlaşma hizmetinin neden güvenli olmadığını
- Yeni ve daha güvenli bir e-posta hesabının nasıl oluşturulacağını
- Halihazırdaki e-posta hesabınızın güvenliğini nasıl arttıracığınızı
- Güvenli bir anlık mesajlaşma hizmetini nasıl kullanılabileceğini
- Birilerinin e-posta hesabınıza eriştiğini düşünüyorsanız ne yapılabileceğini
- Bir e-posta alıcısının kimliğinin nasıl doğrulanacağını

E-postanızı güvenli kılmak

E-posta iletişiminizin güvenliğini arttırmak için atabileceğiniz birkaç önemli adım vardır. Bunlardan ilki verili bir mesajı sadece gönderdiğiniz kişinin okuyabileceğinden emin olmaktır. Bunlar, aşağıda [Webmail'inizin gizliliğini korumak](#) [97] ve [Daha güvenli bir e-posta hesabına geçmek](#) [98] kısımlarında ele alındı. Başlangıç düzeyinin ötesine geçecek olursak, e-posta alıcılarınızın, belirli bir mesajın sizmiştiniz gibi yapan birinden değil de gerçekten sizden geldiğini doğrulayabilmeleri kimi zaman yaşamsal öneme haizdir. Bunu yapmanın bir yolu, [İleri düzey e-posta güvenliği](#) [99]'nin [Bir mesajı şifrelemek ve kimliğini doğrulamak](#) [100] kısmında, ele alınmıştır.

E-posta hesabınızın gizliliğinin ihlal edildiğini düşündüğünüzde ne yapmanız gerektiğini de bilmelisiniz. [E-postaların izlendiğinden şüphe edildiğinde yapabilecekleriniz üzerine ipuçları](#) [101] kısmı bu soruya işaret etmektedir.

Yazdığınız her şey bir casus yazılımla kaydediyor ve düzenli olarak internet üzerinden üçüncü kişilere gönderiliyorsa güvenli e-postanın size bir faydasının olmayacağını da hatırlayın. [Bilgisayarınızı kötü amaçlı yazılımlara ve hacker'lara karşı nasıl korursunuz](#) [56] başlıklı [1. Bölüm](#) [56] bu tür bir şeyden kaçınmak için bazı tavsiyeler sunmaktadır ve [Güvenli şifreler nasıl oluşturulur ve muhafaza edilir](#) [37] başlıklı [3. Bölüm](#) [37], aşağıda ele alınan e-posta ve anlık mesajlaşma araçları için hesaplarınızı korumanıza yardım edecektir.

Webmail'inizin gizliliğini korumak

İnternet açık bir ağıdır ve bu ağ aracılığıyla bilgi okunabilir bir formatta yolculuk eder. Normal bir e-posta mesajı, alıcısına doğru giderken ele geçirilirse içeriği kolayca okunabilir. İnternet, trafiği yönlendirmek için aracı bilgisayarlara tabi olan, bütün dünyaya yayılmış bir büyük ağ olduğundan, birçok farklı kişinin bir mesajı ele geçirmek için fırsatı olabilir. [İnternet Servis Sağlayıcınız ISP](#) [102], alıcısına doğru gezintisine başlarken bir e-posta mesajının ilk alıcısıdır. Benzer bir şekilde alıcınızın [ISP](#) [102]'si, mesajınızın teslim edilmeden önceki son durağıdır. Belirli önlemler almazsanız, mesajınız bu noktalardan herhangi birinde ya da bunların arasındaki herhangi bir noktada okunabilir veya değiştirilebilir.

Pablo: Ortaklarımızdan biriyle bütün bunlar hakkında konuştum ve o bana, o ve meslektaşlarının şifresini paylaştıkları bir webmail hesabının 'Taslaqlar' klasörünün altında önemli mesajlarını kimi zaman kaydettiklerini söyledi. Bu bana garip göründü ama işe yarayabilir mi? Demek istiyorum ki, hiçbir zaman gerçekten gönderilmediğinden, herhangi birinin mesajları okumasını engelleyebilir mi?

Claudia: Bilgisayarında bir e-posta okuduğun her seferinde, okuduğun sadece bir 'taslak' bile olsa, onun içeriği sana internet üzerinden gönderilir. Aksi halde okuduğun mail senin ekranında beliremez değil mi? Öyle ki, birileri seni gözetim altına alıyorsa sadece e-posta mesajlarını izlemiyordur. Bilgisayarına gelen ve bilgisayarından giden tüm okunabilir bilgiyi tarayabilirler. Bir başka deyişle bu taktik, bu paylaşılan webmail hesabına herkes güvenli bir şekilde bağlanmadığı sürece işlemez. Eğer herkes güvenli bağlanıyorsa zaten ayrı hesaplar oluşturmanın ya da "gönder" düğmesine tıklamanın hiçbir sakıncası yoktur.

Bilgisayarınız ile ziyaret ettiğiniz web sitesi arasındaki internet bağlantısını güvenli kılmak uzun zamandan beri olanaklı. Web sitelerine şifreler ya da kredi kartı bilgileri girerken bu güvenlik düzeyiyle sık sık karşılaşsınız. Bunu olanaklı kılan teknoloji, Güvenli Soket Katmanı [SSL](#) [103] [şifreleme](#) [40] olarak adlandırılır. [SSL](#) [103] kullanıp kullanmadığınızı internet tarayıcınızın **adres çubuğuna** yakından bakarak söyleyebilirsiniz.

Normalde tüm web adresleri, aşağıdaki örnekte görülebileceği gibi, **HTTP** harfleriyle başlar:



Güvenli bir web sitesini ziyaret ederken adres **HTTPS** ile başlayacaktır.



Sondaki fazladan **S** bilgisayarınızın web sitesine güvenli bir bağlantı açtığını gösterir. Tarayıcı pencerenizin **adres çubuğunda** ya da alttaki **durum çubuğunda** bir 'kilit' simgesi de görebilirsiniz. Bunlar, internet bağlantınızı izleyebilen herhangi birinin artık iletişiminizi bu bağlantıdığınız web sitesi aracılığıyla izleyemeyeceğini bilmenizi sağlayan ipuçlarıdır.

Şifre ve mali işlemlerinizin korunmasına ek olarak bu tip bir **şifreleme** [104], webmail'inizi güvenli kılmak için mükemmeldir. Bununla birlikte birçok webmail hizmet sağlayıcısı güvenli erişim sunmamaktadır ve bazı webmail hizmetleriye bir seçenek belirterek ya da **HTTPS**'i elle yazarak izin vermenizi talep etmektedir. Siteye giriş yapmadan, e-postanızı okumadan ya da bir mesaj göndermeden önce bağlantınızın güvenli olduğundan daima emin olun.

Güvenli bir webmail hesabına erişmeye çalışırken tarayıcınız aniden geçersiz **güvenlik sertifikalarından** [105] şikâyet etmeye başlarsa dikkatli olmalısınız. Bu, birilerinin mesajlarınızı ele geçirmek için bilgisayarınız ve sunucu arasındaki iletişime müdahale ediyor olduğu anlamına gelebilir. Son olarak hassas bilgi alışverişinde bulunmak için webmail'e başvuracaksanız, tarayıcınızın olabildiğince güvenli olması önemlidir. Mozilla **Firefox** [13]'u ve onun güvenlikle ilgili eklentilerini kurmayı düşünün.

Uygulama: **Eklentileriyle Firefox - Güvenli İnternet Tarayıcısı Rehberi** [14] ile uygulamaya başlayın

Pablo: Bu rapor üzerinde bizimle birlikte çalışacak olanlardan biri iş yerinin dışındayken Yahoo webmail hesabını kullanmayı tercih ediyor. Ve Hotmail kullanan bir başkasını da hatırlar gibiyim. Bu kişilere mesaj gönderirsem başkaları da mesajlarımı okuyabilir mi?

Claudia: Muhtemelen. Yahoo, Hotmail ve diğer birçok webmail hizmet sağlayıcısı, kullanıcı mesajlarının güvenliğini korumayan, güvenli olmayan web sitelerine sahip. Güvenli olarak bu tanıklıkları ele almak istiyorsak bazı kişilerin alışkanlıklarını değiştirmek zorundayız.

Daha güvenli bir e-posta hesabına geçmek

Webmail hizmet sağlayıcılarının çok azı e-postanıza **SSL** [103] erişimi sunmaktadır. Yahoo ve Hotmail, örneğin, sadece giriş yaptığınızda şifrenizi korumak için güvenli bir bağlantı sunmaktadır ancak mesajlarınızın kendisi güvenli olmayan bir şekilde gönderilir ve alınır. Dahası, Yahoo, Hotmail ve diğer ücretsiz webmail hizmet sağlayıcıları gönderdiğiniz bütün mesajlarınıza kullandığınız bilgisayarın **IP adresini** [106] de ekler.

Öte yandan Gmail hesapları giriş yapmanızdan çıkışınıza kadar güvenli bir bağlantı kullanır. Bunu, sürecin başından sonuna kadar adres çubuğuna bakarak ve URL'nin 'https' ile başladığını ('s' burada güvenli bir bağlantıya işaret etmektedir) gözlemleyerek doğrulayabilirsiniz. Yahoo ya da Hotmail'in aksine Gmail, e-posta alıcılarına **IP adresinizi** [106] açık etmekten kaçınır. Ancak hassas e-posta iletişiminizin gizliliği için tamamen Google'a güvenmeniz tavsiye edilmez. Google çok çeşitli nedenlerle kullanıcılarının mesajlarını tarar ve kaydeder; ve geçmişte dijital özgürlüğü sınırlayan hükümetlerin taleplerini yerine getirmişti. Google'ın gizlilik politikası hakkında daha fazla bilgi için **Okuma önerileri** [107] bölümüne bakınız.

Olanaklıysa **https://mail.riseup.net** [108] adresini ziyaret ederek yeni bir RiseUp e-posta hesabı oluşturmalsınız. **RiseUp** [92] dünyanın her yerindeki aktivistlere ücretsiz e-posta hizmeti sunmaktadır ve sunucularında kaydedilen bilginin korunması konusunda büyük çaba sarf etmektedir. Onlar uzun zamandan beri güvenli bir e-posta çözümü arayışında olanlar için güvenilir bir kaynak olmuştur. Ve Google'ın aksine kullanıcılarının gizliliği konusunda oldukça katı politikaları vardır ve bir gün bu politikalarla çatışabilecek hiçbir ticari çıkarları yoktur. Yeni bir **RiseUp** [92] hesabı oluşturmak için iki 'davet kodu'na ihtiyacınız olacaktır. Bu kodlar halihazırda bir **RiseUp** [92] hesabı olan herhangi biri tarafından verilebilir. Bu kitapçığın basılı bir kopyasına sahipseniz, onunla birlikte 'davet kodlarınızı' da almış olmanız gerekir. Aksi halde iki **RiseUp** [92] kullanıcısı bulmanız ve her birine size bir kod göndermesi için sormanız gerekmektedir.

Uygulama: **RiseUp – Güvenli E-posta Hizmeti Rehberi** [109] ile uygulamaya başlayın

Hem Gmail hem de **RiseUp** [92] bir webmail hizmeti sağlayıcısından daha fazlasıdır. Onlar, **İleri düzey e-posta güvenliği** [99] başlığı altında betimlenen teknikleri destekleyen Mozilla **Thunderbird** [69] gibi bir e-posta istemcisiyle birlikte de kullanılabilir. E-posta istemcinizin e-posta sağlayıcınızla **şifrelenmiş** [40] bir bağlantı yaptığından emin olmak, webmail'inize **HTTPS** ile erişmek kadar önemlidir. Bir e-posta istemcisi kullanıyorsanız ek ayrıntılar için **Thunderbird Rehberi** [70]'ne bakınız. En azından, hem gelen hem de giden e-posta sunucularınız için **SSL** [103]'e ya da **şifrelemeye** [40] izin verdiğinizden emin olun.

Pablo: Öyle ise RiseUp kullanmaya mı başlamalıyım yoksa sadece güvenli 'https' adresine geçerek Gmail kullanmaya devam edebilir miyim?

Claudia: Bu sana kalmış ama bir e-posta hizmet sağlayıcısı seçerken kesinlikle göz önünde bulundurman gereken birkaç şey var. Birincisi, hesabına güvenli bir bağlantı sunuyor mu? Gmail sunuyor, o zaman Gmail tamam. İkincisi, hizmet yöneticilerinin e-postalarını gizli tutacaklarına ve okumayacaklarına ya da onları başkalarıyla paylaşmayacaklarına güveniyor musun? Buna sen karar vereceksin. Ve son olarak bu sağlayıcıyla özdeşleşmenin kabul edilebilir olup olmadığını düşünmen gerekir. Bir başka deyişle aktivistler arasında popüler olan, sonu 'riseup.net'le biten bir e-posta

adresini kullanman başına iş açar mı yoksa daha yaygın kullanımı olan 'gmail.com' adresini kullanmak mı ihtiyacını karşılar?

Hangi güvenli e-posta araçlarını kullanmaya karar vermenizden bağımsız olarak, her mesajın bir göndereni ve bir ya da daha fazla alıcısı olduğunu göz önünde bulundurun. Siz sadece resmin bir parçasısınız. E-posta hesabınıza güvenli olarak erişseniz bile bağlantıda olduğunuz kişilerin mesaj gönderirken, okurken ve yanıtlarken hangi önlemleri aldığını ya da almadığını düşünün. Yazıştığınız kişilerin e-posta sağlayıcılarının nerede konumlandığını öğrenmeye çalışın. Doğal olarak bazı ülkeler e-postaları izlemek konusunda diğerlerine göre daha saldırgandır. **Özel iletişimi güvence altına almak için siz ve yazıştığınız kişilerin tümü görece güvenli ülkelerde tutulan güvenli e-posta hizmetleri kullanmalısınız.** Ve mesajlarınızın e-posta sunucunuz ve alıcının e-posta sunucusu arasında ele geçirilmediğinden emin olmak için aynı sağlayıcıdan hesaplar seçmelisiniz. RiseUp [92] iyi bir seçimdir.

E-posta güvenliğinizi arttırmak için ek ipuçları

- Beklemediğiniz, bilmediğiniz birinden gelen ya da şüpheli konu satırı içeren e-postaların eklerini açarken daima dikkatli olun. Bu tür e-postaları açarken anti-virüs yazılımınızın güncel olduğundan emin olun ve tarayıcınızın ya da e-posta programınızın gösterdiği herhangi bir uyarıya dikkat edin.
- İnternette nasıl anonim kalınır ve internet sansürü nasıl aşılr** [110] başlıklı **8. Bölüm** [110]'de anlatılan *Tor* [111] gibi anonimlik yazılımlarını kullanmanız seçtiğiniz e-posta hizmetini, internet bağlantınızı izliyor olabilecek herhangi birinden gizlemenize yardım edebilir. Ülkenizdeki internet filtrelemesinin boyutlarına bağlı olarak, RiseUp [92] ya da Gmail güvenli e-posta sağlayıcılarına erişmek için dahi, *Tor* [111] ya da **8. Bölüm** [110]'de anlatılan diğer sansür aşma [112] araçlarından birini kullanmanız gerekebilir.
- E-posta alıcılara ya da e-posta aracılığıyla mesaj gönderebileceğiniz genel forumlara anonim kalmak amacıyla kullanmak istediğiniz bir hesap oluştururken, kendi kişisel ya da meslekî yaşamınızla ilişkisi olan bir kullanıcı adı ya da ad ve soyadla kayıt yaptırmamaya dikkat etmelisiniz. Bu tür durumlarda, gönderdiğiniz mesaja IP adresinizi [106] ekleyen Hotmail, Yahoo ve herhangi bir diğer webmail sağlayıcısını kullanmaktan kaçınmanız da önemlidir.
- Bilgisayarınıza fiziksel olarak kimlerin eriştiğine bağlı olarak, geçici dosyalarınızdan e-posta ilişkili izleri temizlemek, mesajlarınızı internette yol alırken korumak kadar önemli olabilir. Ayrıntılar için Hassas bilgiler nasıl imha edilir [61] başlıklı **6. Bölüm** [61]'e ve Cleaner Rehberi [86]'ne bakınız.
- Bağlantıda olduğunuz kişilerin oluşturduğu ağı korumak amacıyla farklı gruplarla haberleşmek için birden fazla farklı, anonim e-posta hesabı kullanmayı düşünebilirsiniz. Kaydolmak için e-posta hesabı gerektiren internet servisleri için farklı farklı e-posta hesapları kullanabilirsiniz.
- Yukarıda verilen bütün önlemleri aldıktan sonra bile mesajlarınıza ne yazdığınıza çok dikkat etmek ve mesajlarınızın yanlış ellere geçmesi durumunda bunun nasıl bir etkisi olacağını iyi değerlendirmek hâlâ çok önemlidir. Değiş tokuş edilen bilginin güvenliğini artırmanın bir yolu, hassas bilgileri değiş tokuş ederken insanların gerçek isimlerini, yerlerin gerçek adresini vb. kullanmayacağınız bir kod sistemi geliştirmektir.

E-postaların hack'lendiğinden ya da izlendiğinden şüphe edildiğinde yapabilecekleriniz üzerine ipuçları

E-posta hesabınızın hack'lendiğinden ya da gizliliğinin ihlal edildiğinden şüphe ediyorsanız, yapılan hasarı azaltmak için bazı önlemler alabilirsiniz. Hesabınızın hack'lendiğinden emin olmak zor olsa da, aşağıda verilenler hesabınızın gizliliğinin ihlal edildiğini gösteren bazı ip uçlarıdır:

- e-posta hesabınızın içeriği ya da ayarlarında sizin yapmadığınız bazı değişiklikler fark etmeniz;
- e-posta kontaklarınızın sizin göndermediğiniz bir mesajı aldıklarını size bildirmesi;
- şifrenizin ve diğer ayarlarınızın doğru olduğundan emin olmanıza rağmen e-posta hesabınıza oturum açamıyorsanız;
- iş arkadaşlarınızın gönderdiği e-posta mesajlarını düzenli olarak almıyorsanız;
- sadece e-posta ile gönderilen ya da alınan şahsi bir bilginin, siz ya da yazıştığınız kişi tarafından başkasıyla paylaşılmamış olmasına rağmen, üçüncü şahısların bilgisi dahiline geçmesi;
- hesabınızın etkinlik geçmişinde (e-posta sağlayıcınız bu özelliği sağlıyorsa), hatırlamadığınız bir zamanda veya gitmediğiniz bir yerden (ya da IP adresinden) hesabınıza ulaşıldığını görmeniz.

Bu gibi durumlarda bazı önlemler almak isteyebilirsiniz:

- Bahsi geçen e-posta hesabınızdan hassas bilgiler paylaşmayı bırakın**, en azından durumu daha iyi anlayana kadar.
- Şifrenizi en kısa zamanda değiştirin.** Bakınız: **Bölüm 3. Güvenli şifreler nasıl oluşturulur ve muhafaza edilir** [37]. Hesabınızın (ya da diğer hesaplarınızın) şifresini değiştirebilmek için, e-posta sisteminizde nasıl şifre değiştirildiğini önceden bilmeniz gerekir, böylece gerektiğinde hızlıca uygulayabilirsiniz. **Aynı ya da benzer şifreyi kullandığınız diğer hesaplarınızın şifresini değiştirin**; çünkü bu hesapların da gizliliği ihlal edilmiş olabilir. Her hesap için farklı ve güçlü şifreler kullanın. Diğer bütün hesaplarınızın şifrelerini değiştirmek isteyebilirsiniz. Şifrelerinizi saklamak ve idare etmek için KeePass [52] kullanmayı göz önünde bulundurun. Bütün hesaplarınızın **güvenlik sorularının cevaplarını değiştirin** (eğer kullanıyorsanız); böylece başkaları tarafından tahmin edilmesini ya da hakkınızda araştırma yapılarak cevapların bulunmasını imkansız kılın. Bu, bilgisayarınıza casus yazılım bulaşması ve dolayısıyla hesaplarınızın riske atılmış olması durumuna karşı bir ön tedbirdir.
- Eğer şifrenizi değiştirmek için **hesabınıza oturum açamıyorsanız**, e-posta sağlayıcınızla kontağa geçip hesabınızın iadesini istemeyi deneyin. Bu durumlarda kullanıcılara yardımcı olmak için bazı e-posta sağlayıcılarının özel

prosedürleri vardır. Bu prosedürlerin içeriğini, bu gibi durumlarla karşılaşmadan önce bilmek faydalıdır.

- **Bilgi kaybını ve bunun tanındıklarınız üzerindeki etkisini azaltın.** Bir eylem planı yapmak önemlidir. Hesabınızda ne tür hassas bilgilerin olduğunu bilmek ve kimlerle bu hesaptan bilgi paylaştığınızı tespit etmek, kimi uyarmanız gerektiğine karar vermek ve hangi diğer hesapları tekrar ziyaret edeceğinize ya da kapatacağınıza karar vermek. Hangi servisleri (web, finansal, vb.) tekrar ziyaret etmek ya da kapatmak zorunda olduğunuzu kararlaştırın. **Hesap dosyalarını kontrol etmeniz** (eğer mümkünse), hesabınızdan nelerin gönderilmiş olabileceğini araştırmak ve ona göre hareket etmek için önemlidir. **Kontaklarınızı haberdar etmek** için kontak kişilerinizin ayrı bir yedek kopyasını tutmanıza ihtiyacınız olacak. Ayrıca, yapılmış olabilecek değişiklikleri görmek için, **hesap ayarlarınızı yeniden gözden geçirin.** Bağlantılar ve kötü amaçlı yazılımlar için e-posta imza ayarlarını; almış olduğunuz e-mailleri kopyalayarak üçüncü kişilere gönderilmesini sağlayan e-posta forward ayarlarını ve otomatik cevap mesajları, görünen ad gibi diğer ayarları kontrol edin.
- **Hesabınızın gizliliğinin nasıl ihlal edildiğini araştırın.** Zayıf bir şifreniz olduğundan mı, yoksa casus yazılım bulaşmasından mı, gibi. Bu konuda ne kadar çok bilgi sahibi olursanız, duruma o kadar iyi müdahale edebilir ve kontaklarınızı koruyabilirsiniz.
- **Bu hesaptan e-postalarınıza erişen bütün araçların, ve bu hesabınızın şifrelerini muhafaza ettiğiniz araçların güvenliğini yeniden gözden geçirin.** Bakınız: **1. Bilgisayarınızı kötü amaçlı yazılımlara ve hacker'lara karşı nasıl korursunuz** [56], **2. Fiziksel tehditlere karşı bilgilerinizi nasıl korursunuz** [57] ve **11. Akıllı telefonlar nasıl olabildiğince güvenli kullanılır** [113]. Anti-virüs yazılımınızı gözden geçirin (bakınız: **Avast! - Anti-Virüs** [9] ve **Spybot - Anti-Casus Yazılı** [12] uygulamalı rehberler). Bilgisayarınızı tarayın: **4.1 Virüs Salgınlarıyla Baş Etmek için Kısa Rehbe** [114] kısmını okuyun. Eksiksiz bir tarama için kurtarma CD'si ya da USB kullanın - **4.9 İleri Düzey Virüs Temizleme Metotları** [115] kısmını okuyun. Aracınızı temizleyebileceğinizden emin değilseniz, temiz bir kaynaktan işletim sisteminiz dahil bütün yazılımları yeniden yükleyin. **Firefox** [14], **Thunderbird** [70], **LibreOffice** [116] ve diğer **Ücretsiz ve Açık Kaynak Kodlu Programlar** [7] gibi daha güvenli programlara geçmeyi değerlendirin. Yukarıda verilenleri yaptıktan sonra, hesap şifrelerinizi yeni, daha güçlü şifrelerle tekrar değiştirin.
- E-posta sağlayıcınıza hesabınızın hack'lendiğini rapor etmeyi gözden geçirin.
- Farklı, daha güvenli bir hesap kullanmayı değerlendirin, örneğin, sıra dışı yer ve araçlardan erişimi engelleyen ya da böyle bir erişim söz konusu olduğunda size haber veren bir hesap. Ülkenizin dışında 'host' edilen bir hesabı kullanmayı değerlendirin. E-posta şifrelemesi kullanmayı düşünün – **pgp4usb - e-posta metni ve dosya şifreleme** [117] ya da **Enigmail ve GPG ile Thunderbird – Güvenli E-posta İstemcisi** [70].
- Okunmuş e-postaları, e-posta hesabınızın sunucusunda depolamaktan kaçınmayı göz önünde bulundurun. Bunun yerine, okunmuş e-postalarınızı güvenliği sağlanmış bilgisayarınıza yükleyin. Hesabınıza bağlanma şeklinizin ve bunu yaparken kullandığınız araçların güvenliğini analiz edin.

Bunun gibi bir durumda hızlı ve doğru şekilde hareket etmeniz önemli. Önceden hazırlanmış ve prova edilmiş bir plan size yardımcı olabilir.

Birilerinin halihazırda e-postalarınızı izlediğinden şüpheleniyorsanız yeni bir hesap oluşturmak ve eskisini yem olarak saklamaya devam etmek isteyebilirsiniz. Bununla beraber, geçmişte e-posta alışverişinde bulunduğunuz herhangi bir hesabın şu anda izleniyor olabileceğini de hatırlayın. Sonuç olarak bazı ek önlemleri dikkatle takip etmelisiniz:

- Hem siz hem de geçmişte yazıştığınız kişiler yeni hesaplar oluşturmali ve bu hesaplara sadece, internet kafeler gibi daha önce hiç kullanmadığınız yerlerden bağlanmalısınız. Bu stratejiyi, normalde kullandığınız ve izlenme ihtimali olan bilgisayarınızdan yaptığınız bağlantıların yeni hesabınızın konumunu ele vermesini engellemek için öneriyoruz. Alternatif olarak, yeni hesabınıza normal konumunuzdan giriş yapmak zorundaysanız bu bağlantıları gizlemek için **İnternette nasıl anonim kalınır ve internet sansürü nasıl asılır** [110] başlıklı **8. Bölüm** [110] de anlatılan araçlardan birini kullanabilirsiniz.
- Bu yeni e-posta adresleriyle ilgili bilgiyi sadece, yüz yüze toplantılar, güvenli anlık mesajlar ya da şifrelenmiş **VoIP** [91] iletişimi gibi, güvenli kanalları kullanarak paylaşın.
- En azından bir süre için eski hesabınızdaki trafiği büyük ölçüde değiştirmeden koruyun. Bu, sizi izleyenlere bu hesabı hâlâ hassas haberleşmeleriniz için kullanıyormuşsunuz gibi görünmenizi sağlar. Varsayımsal olarak kritik bilgileri açığa vurmaktan kaçınmak isteyeceksiniz ama böyle yaptığınızı fark ettirmemeye çalışmalısınız. Hayal edebileceğiniz gibi bu bir parça zorlu bir iştir.
- Gerçek kimliğinizle yeni hesabınız arasında bağlantı kurulmasını güçleştirin. Yeni hesabınızdan eskisine ya da eskisinden yenisine (ya da izlenebileceğini düşündüğünüz diğer kişilerin hesaplarına) e-posta göndermeyin.
- Yeni hesabınızı kullanırken ne yazdığınıza dikkat edin. Gerçek adlarla adresleri ve 'işkence' gibi ifadeleri kullanmaktan kaçınmanız en iyisidir. Yazıştığınız kişilerle resmi olmayan bir kod sistemi geliştirin ve bunu düzenli olarak değiştirin.
- E-posta güvenliğinin sadece güçlü teknik savunmalarla ilgili olmadığını hatırlayın. E-posta güvenliği, sizin ve yazıştığınız kişilerin birbirinizle nasıl iletişim kurduğunuza gösterdiğiniz dikkatle ve teknik olmayan güvenlik alışkanlıklarınızın disiplinli olmasıyla ilişkilidir.

Diğer internet iletişim araçlarını güvenli kılmak

E-postaya benzer bir biçimde anlık mesajlaşma ve **VoIP** [91] yazılımı, seçtiğiniz araçlara ve onları nasıl kullandığınıza bağlı olarak güvenli ya da güvensiz olabilir.

Anlık mesajlaşma yazılımınızı güvenli kılmak

'Sohbet/chat' olarak da adlandırılan anlık mesajlaşma, normalde güvenli değildir ve e-posta kadar izlenmeye açık olabilir. Sohbet oturumlarınızın gizliliğini güvenlik altına almaya yardım edebilecek programlar bulunmaktadır. Ancak e-postalarda olduğu gibi, güvenli bir iletişim kanalı hem sizin hem de anlık mesajlaştığınız kişilerin aynı yazılımı kullanmasını ve aynı güvenlik önlemlerini almasını gerektirir.

Var olan birçok anlık mesajlaşma protokolünü destekleyen, hesap adınızı değiştirmek ya da bağlantıda olduğunuz kişiler listesini yeniden oluşturmak zorunda kalmaksızın kolayca kullanmaya başlayabileceğiniz, *Pidgin* [93] adı verilen bir sohbet programı bulunmaktadır. *Pidgin* [93] aracılığıyla özel ve *şifrelenmiş* [40] konuşmalar yapmak için *Off the Record OTR* [94] eklentisini kurmanız ve aktif hale getirmeniz gerekmektedir. Bu oldukça basit bir süreçtir.

Uygulama: *OTR eklentili Pidgin – Güvenli Anlık Mesajlaşma Rehberi* [118] ile uygulamaya başlayın

Pablo: Yahoo webmail servisi güvensizse bu Yahoo Sohbet'in de güvensiz olduğu anlamına mı geliyor?

Claudia: Hatırlanması gereken şey, anlık mesajlaşmayı bu raporu tartışmak için kullanmak istiyorsak bu işe dahil olan herkesin Pidgin ve OTR yazılımlarını yüklemiş olduğundan emin olmak. Yüklemişlerse Yahoo Sohbet ya da diğer sohbet hizmetlerini kullanabiliriz.

VoIP yazılımınızı güvenli kılmak

Diğer *VoIP* [91] kullanıcılarıyla yapılan *VoIP* [91] görüşmeleri genelde ücretsizdir. Bazı programlar uluslararası numaralar dahil, telefonlarla da ucuz görüşmeler yapmanıza izin verebilir. Bu özelliklerin çok yararlı olduğunu söylemeye gerek bile yok. *Skype* [119] (aşağıya bakınız), *Jitsi* [120], *Google Talk* [121], *Yahoo! Voice* [122], ve *MSN Messenger* [123], günümüzün daha popüler *VoIP* [91] programlarından bazılarıdır.

Normal olarak, internet üzerinden sesli iletişim korumasız e-posta ve anlık mesajlaşmadan daha güvenli değildir. Hassas bilgileri paylaşmak için sesli iletişimi kullanırken bilgisayarınızdan alıcının bilgisayarına kadar olan yol boyunca görüşmenizi şifreleyen bir araç seçmek önemlidir. Güvenilir bir topluluk tarafından gözden geçirilmiş, sınanmış ve tavsiye edilmiş Ücretsiz ve Açık-Kaynak Kodlu bir Yazılımı kullanmak en iyisi olacaktır. Yukarıdaki kriterleri göz önünde bulundurarak VoIP seçiminizi olarak *Jitsi* [120]'yi denemenizi öneriyoruz.

Skype'in güvenliği hakkında uyarı

Skype [34] sabit ve cep telefonlarını aramayı da destekleyen, oldukça yaygın olarak kullanılan bir anlık mesajlaşma ve VoIP aracıdır. Popülerliğine rağmen birçok sorun bu yazılımı güvenli bir seçim olmaktan çıkarır. Bu sorunlardan bazıları aşağıda tanımlanmıştır.

Skype'a göre o hem mesajları hem de sesli aramaları *şifrelemektedir* [40], bu sadece iletişimin her iki tarafının da Skype programı kullanması durumunda gerçekleşir. Skype telefon aramalarını ve SMS mesajları olarak gönderilen metinleri şifrelememektedir.

İletişimin her iki tarafı da (orijinal) Skype programı kullanıyorsa, Skype görüşmesinin şifrelenmesi onu, telefon üzerinden yapılan sıradan bir aramadan görünüşte daha güvenli kılmaktadır. Ama Skype'ın kapalı-kaynak kodlu bir program olması, bağımsız bir denetimi ve şifreleme konusundaki iddialarının değerlendirilmesini olanaksız kılmaktadır. Bu nedenledir ki Skype'ın kullanıcılarını, kullanıcıların bilgilerini ve iletişimini ne kadar iyi koruduğunu doğrulamak olanaksızdır. ***Bilgisayarınızı kötü amaçlı yazılımlara ve hacker'lara karşı nasıl korursunuz*** [56] başlıklı **1. Bölüm** [56]'ün ***Yazılımlarınızı güncel tutmak*** [124] kısmı, ***Ücretsiz ve Açık-Kaynak Kodlu Yazılım FOSS*** [7]'ün erdemlerine işaret eder.

Daha öncede belirtildiği gibi, güvenli bir iletişim aracı olarak her ne kadar Skype'ı tavsiye edemiyorsak da, hassas iletişimlerin için bir araç olarak Skype'ı kullanmaya yine de karar veriyorsanız bazı önlemler almanız önemlidir:

- Casus yazılım bulaşmış bir Skype programından kaçınmak için, Skype'ı sadece resmî web sitesinden, www.skype.com [119], indirin ve kurun. URL'yi daima iki kez kontrol etmek resmî siteye bağlandığınızdan emin olmak için önemlidir. Bazı ülkelerde Skype web sitesi engellenmiştir ve/veya Skype'ın resmî sitesi olduğunu iddia eden birçok sahte site bulunmaktadır. Bu tür birçok durumda, erişilebilir durumdaki Skype sürümlerine, herhangi bir iletişimi izlemek için tasarlanmış kötü amaçlı yazılımların bulaşmış olması olasıdır. Yazılımın en son sürümünü kurmak ya da bir üst sürüme geçmek istediğiniz her seferinde, Skype web sitesine bağlanmak için **8. Bölüm** [110]'de açıklanan sansür aşma araçlarını kullanın ve orijinal bir Skype programı indirin.
- Düzenli aralıklarla Skype şifrenizi değiştirmeniz önemlidir. Skype farklı konulardan çoklu girişe izin vermektedir ve eş zamanlı oturumların sayısı hakkında size bilgi vermemektedir. Bu büyük bir risk taşımaktadır, şifreniz tehlikeye bu şifreyle herhangi biri de giriş yapabilir. Giriş yapılan oturumlar, tüm yazılı mesajlara ve arama geçmişine erişimi de elde eder. Şifre değiştirmek bu tür düzenbaz oturumları (yeniden giriş yapmaya zorlayarak) engellemenin tek yoludur.
- Skype'ın gizlilik ayarlarını sohbet geçmişini saklamayacak şekilde değiştirmek de tavsiye edilebilir.
- Skype'ın gelen dosyaları otomatik olarak kabul etme ayarlarını kapatmanız tavsiye edilir. Öyle ki bu yöntem zaman zaman kötü amaçlı/casus yazılımları bilgisayarınıza bulaştırmak için kullanılır.
- İletişimde olduğunuz kişinin kimliğini daima bağımsız olarak doğrulayın. Konuşmak istediğiniz kişiyi tanıyorsanız, sesli sohbet sırasında bunu yapmak kolaydır.
- Skype kullanıcı adınızın gerçek adınızla ya da kuruluşunuzun adıyla aynı ya da onunla herhangi bir ilişkisinin olup olmaması gerektiğine karar verin.
- Daima alternatif iletişim yollarına sahip olun –Skype her an kullanılamaz hale gelebilir.
- Ne söylediğinize dikkat edin -spesifik bir terminoloji kullanmaksızın hassas konuları tartışmak için bir kodlama

sistemi geliştirin.

Skype'ın popülerliğine rağmen, yukarıda değinilen kaygılar, güvenli bir deneyim için onu tartışmalı hale getirir. VoIP için Jitsi'yi ve güvenli anlık mesajlaşma için [OTR](#) [94] eklentisiyle [Pidgin](#) [93]'i kullanmaya başlamanızı öneriyoruz.

İleri Düzey E-posta Güvenliği

Aşağıda tartışılan araçlar ve kavramlar deneyimli bilgisayar kullanıcılarına tavsiye edilir.

E-postada Açık Anahtar Şifrelemesini Kullanmak

Güvenli olmayan e-posta hesaplarıyla bile daha üst düzey bir e-posta güvenliği elde etmek olanaklıdır. Bunu yapmak için açık anahtar [şifrelemesini](#) [40] öğrenmeniz gerekir. Bu teknik her özgün mesajı kodlayarak mesajınızı göndermek istediğiniz kişi haricinde herkese okunmaz kılar. Açık anahtar [şifrelemesini](#) [40] hünarlı yönü şudur: bağlantıda olduğunuz kişilerle gelecekte mesajlarınızı nasıl şifreleyeceğiniz konusunda herhangi bir gizli bilgi alışverişinde bulunmak zorunda olmazsınız.

Pablo: Ama bu nasıl çalışıyor?

Claudia: Matematik! Bir e-posta alıcısının özel açık anahtarını kullanarak o kişiye yollamak istediğin e-posta'yı kodlarsın. Açık anahtar özgürce dağıtılabilir. Ardından alıcı, gelen mesajlarını okumak için dikkatle korumak zorunda olduğu gizli 'özel anahtarı'nı kullanır. Sırası gelince o kişi, sana yazdıklarını şifrelemek için senin açık anahtarını kullanır. Sonuç olarak açık anahtarlarını değiş tokuş etmek zorundasınız, ama anahtarlarınızı, bunları elde etmek isteyen herhangi biri için endişelenmeksizin, herkese açık bir biçimde paylaşabilirsiniz.

Bu teknik, herhangi bir e-posta servisiyle birlikte, hatta güvenli iletişim kanalları olmayanlarla bile, kullanılabilir çünkü her bir mesaj bilgisayarınızı terk etmeden önce [şifrelenir](#) [40].

[Şifreleme](#) [40] kullanarak dikkatleri üzerinize çekebileceğinizi hatırlayın. Bir webmail hesabı dahil, güvenli bir internet sitesine erişirken kullandığınız [şifrelemenin](#) [40] türü, burada tartışılan açık anahtar [şifrelemesi](#) [40] türüne göre daha az şüpheli görülür. Bazı durumlarda, bu tür [şifrelenmiş](#) [40] veri içeren e-postalar ele geçirilir ya da [şifrelenmiş](#) [40] e-postalar açık bir foruma gönderilirse, bu durum, bunları gönderen kişiyi mesajın içeriğinden bağımsız olarak, suçlu durumuna düşürebilir. Bazen mesajınızın gizliliği ile dikkat çekmeme gereksinimi arasında seçim yapmak zorunda kalabilirsiniz.

Bir Mesajı Şifrelemek ve Kimliğini Doğrulamak

Açık anahtar [şifrelemesi](#) [40] ilk bakışta karmaşık görünebilir ama temel ilkeleri anladığınızda oldukça kolaydır ve araçları kullanmak da zor değildir. Basit, kullanıcı dostu ve taşınabilir [pgp4usb](#) programı, internete bağlı olmasanız bile e-posta mesajlarını ve dosyaları şifreleyebilir.

Uygulama: [Taşınabilir pgp4usb – E-posta metinleri ve dosya şifreleme programı rehberi](#) [117] ile uygulamaya başlayın

Mozilla Thunderbird [69] e-posta programı **Enigmail** [95] adı verilen uzantısıyla birlikte e-posta mesajlarını şifrelemede ve onların şifresinin çözülmesinde kolayca kullanılabilir.

Uygulama: [Enigmail ve GPG ile Thunderbird - Güvenli E-posta İstemcisi Rehberi](#) [70] ile uygulamaya başlayın

VaultletSuite 2 Go [125], ücretsiz şifrelenmiş e-posta programını kullanmak, programı sağlayan şirkete güvenmeye ve sizin için işlerin bir kısmını yapmalarına izin vermeye istekliyseniz, **Thunderbird**'den bile daha kolaydır.

Uygulama: [VaultletSuite 2Go – Güvenli E-posta İstemcisi Rehberi](#) [126] ile uygulamaya başlayın

E-postanızı otantikleştirmek iletişim güvenliğinin bir başka önemli boyutudur. İnternet bağlantısına ve doğru araçlara sahip olan herhangi biri sizinkiyle aynı olan sahte bir e-posta hesabından mesaj göndererek sizi taklit edebilir. Buradaki tehlike alıcının bakış açısından ele alındığında daha görünürdür. Güvenilir bir bağlantıdan geliyormuş gibi görünen ama gerçekte etkinliklerinizi kesintiye uğratmak ya da örgütünüz hakkındaki hassas bilgileri öğrenmek isteyen biri tarafından gönderilen bir e-postanın ortaya koyduğu tehdidi hayal edin.

E-postayla yazıştığımız kişiyi görmeyeceğimizi ya da duyamayacağımızı göz önünde bulundurduğumuzda, kişinin kimliğini doğrulamak için genellikle göndericinin adresine başvururuz, bu nedenledir ki sahte e-postalarla bu kadar kolay aldatılırız. Açık anahtar [şifrelemesine](#) [40] dayanan [dijital imzalar](#) [127], bir mesaj gönderirken birinin kimliğini doğrulamanın daha güvenli bir aracını sağlar. [Portable pgp4usb](#) [117] rehberi ya da [Thunderbird Rehberi](#) [70]'nin [Enigmail'la birlikte Thunderbird nasıl kullanılır](#) [128] kısmı bunun nasıl yapılacağını ayrıntılarıyla açıklar.

Pablo: Bir meslektaşım benim e-posta adresimden gönderilen ama aslında benim göndermediğim bir e-posta almıştı. Sonunda bunun sadece bir spam olduğuna karar verdik ama şimdi yanlış zamanda, yanlış bir kişinin e-posta kutusunda sahte bir e-postanın belirmesinin ne büyük bir hasar meydana getirebileceğini hayal edebiliyorum. Bu tür şeylerin dijital imza ile önlenilebildiğini duydum ama nedir bu dijital imza?

Claudia: Bir dijital imza, mektubunu taşıyan zarfın üzerindeki bal mumundan mühüre benzer ancak dijital imza taklit edilemez. Bu, mesajın gerçek göndericisinin sen olduğunu ve mesajın, alıcısına erişinceye dek değiştirilmediğini kanıtlar.

Okuma önerileri

- E-posta kimlik sahtekarlığı hakkında daha fazla şey öğrenmek için, [Digital Security and Privacy for Human Rights Defenders](#) [25] kitabının 2.5 *Spoofing* bölümüne bakınız.
- Riseup* ve *Thunderbird* Uygulama Rehberlerine ek olarak, mesajlarınızın bir kopyasını e-posta sunucusunda bırakarak, e-posta programınızı çeşitli popüler e-posta hizmet sağlayıcılarıyla birlikte kullanmayı açıklayan bir dizi web sitesi bulunmaktadır:
 - The Riseup web sitesi [129]
 - Gmail kullanma [130] talimatları.
 - Gmail adres defterinizdekileri Thunderbird'e nasıl aktarırsınız [131]
 - Diğer e-posta hizmetlerini bu şekilde kullanmak için, e-posta hizmeti sağlayıcısının web sitesini 'POP', 'IMAP' ve 'SMTP' gibi anahtar sözcüklerle tarayın.
- Man in the Middle attack* [132] olarak bilinen SSL güvenliğine yapılmış bir saldırı bulunmaktadır.
- Bir Gmail hesabı oluştururken kabul etmek zorunda olduğunuz [Gmail Gizlilik Politikası](#) [133], "Google Gmail hesabınızı ve içeriğini, size Gmail hizmeti sunmak için ve hizmetlerini geliştirmek için sürdürür ve işler." demektedir. Gerçekten de tüm e-posta sağlayıcıları, spam karşıtı hizmetlerini ve diğer benzer özelliklerini sağlayabilmek için mesajlarınızı tarar. Bununla beraber Gmail, e-postanızın gerçek içeriği üzerine temellenen 'hedeflenmiş reklamcılığı' sunabilmek için bu konuda biraz daha ileri gider. Bu, Google tarafından depolanan bilginin kasıtlı olarak ya da kazara açığa çıkması durumunda tehlikeli olabilir.
- 2008 yılında yapılan bir dizi söyleşi birçok önde gelen anlık mesajlaşma hizmetinin [gizlilik ve şifreleme politikalarına](#) [134] işaret etti.

8. İnternette nasıl anonim kalınır ve internet sansürü nasıl aşılr

Tüm dünyada birçok ülke, ülkelerindeki internet kullanıcılarının belirli sitelere ve internet hizmetlerine erişimini engelleyen yazılımlar kurdu. Şirketler, okullar, ve halka açık kütüphaneler; çalışanlarını, öğrencilerini ve abonelerini rahatsız edici ya da zararlı olduğunu düşündükleri materyallere karşı korumak için sık sık benzer yazılımlar kullanır. Bu türden bir filtreleme teknolojisinin bir dizi farklı türü vardır. Bazı filtreler bir siteyi [IP adresi](#) [106] üzerinden engellerken diğerleri belirli [alan adlarını](#) [135] kara listeye alır ya da tüm şifrelenmemiş internet iletişimini belirli anahtar sözcüklere bakarak tarar.

Hangi filtreleme yönteminin mevcut olduğundan bağımsız olarak, ülkenizin dışındaki aracı bilgisayarlara sizin için engellenmiş hizmetlere erişmesi için itimat ederek, bu filtreleme yöntemlerini aşmak neredeyse her zaman olanaklıdır. Bu süreç, [sansür aşma](#) [112] olarak adlandırılır ve aracı olan bilgisayarlar da [proxy](#) [136]'ler olarak adlandırılır. [Proxy](#) [136]'lerin de farklı türleri vardır. Bu bölüm önce, çoklu-proxy anonimlik ağları üzerine kısa bir tartışmayı ele alacak; ardından da temel [sansür aşma](#) [112] [proxy](#) [136]'lerine ve onların nasıl çalıştığına dair daha ayrıntılı bir açıklamaya geçecektir.

İnternet filtrelerini aşmak için her iki yöntem de etkilidir ancak ilki, internet etkinliklerinizi olabildiğince anonim kılmak için internet hızınızdan ödün vermeye istekliyseniz yerinde bir seçimdir. [Proxy](#) [136]'nizi yöneten kişilere ve kuruluşlara güveniyorsanız ve performans sizin için anonimlikten daha önemliyse, temel bir [sansür aşma](#) [112] [proxy](#) [136]'si size daha iyi bir hizmet sunabilir.

Arka plan senaryosu

Mansour ve Magda Arapça konuşulan bir ülkede yaşayan kardeşlerdir. Anonim olarak insan hakları ihlallerini yayınladıkları ve siyasal değişim için bir kampanya yürüttükleri bir blogları vardır. Ülkelerindeki yetkililer, web sitelerinin sunucusu başka bir ülkede konuşlandığından sitelerini kapatamamıştır; ancak diğer etkinliklerinden yola çıkarak blog'un yöneticileri hakkında sık sık daha çok şey öğrenmeye çalışmaktadırlar. Mansour ve Magda yetkililerin güncellemelerini izleyebileceğinden ve kim olduklarını bulabileceklerinden kaygı duymaktadır. Dahası sadece web sitesini güncellemeye devam edebilmek için değil; aynı zamanda kendi ülkelerindeki okuyucularına sansür aşmak için gerekli uygun önerilerde bulunmak için, hükümetin eninde sonunda web sitelerini filtreleyeceği güne hazırlanmak istemektedirler.

Bu bölümden ne öğrenebilirsiniz

- Kendi ülkenizin içinden engellenmiş bir web sitesine nasıl erişileceğini
- Ziyaret ettiğiniz web sitelerinin konumunuzu bilmesini nasıl engelleyeceğinizi
- Sizin [ISP](#) [102]'nizin ya da ülkenizdeki herhangi bir izleme/denetleme organının, sizin hangi web sitesini ya da internet hizmetini ziyaret ettiğinizi tespit etmesini nasıl engelleyeceğinizi

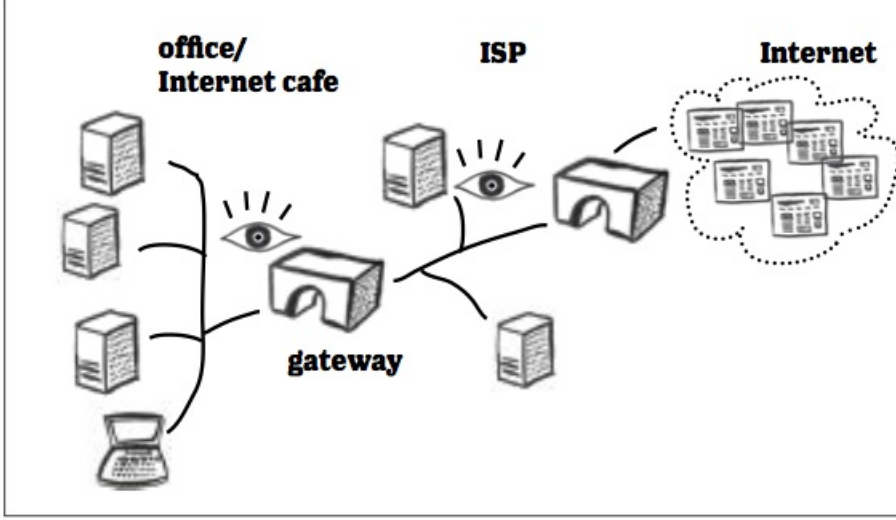
İnternet sansürünü anlamak

[OpenNet Initiative \(ONI\)](#) [137] ve [Reporters Without Borders \(RSF\)](#) [138] gibi örgütler tarafından gerçekleştirilen araştırmalar, birçok ülkenin sosyal, siyasal ve 'ulusal güvenlik' gibi oldukça çeşitli içerikleri filtrelediğine; ancak bu ülkelerin nadiren neyin engellendiğinin kesin listesini yayınladığına işaret etmektedir. Doğal olarak yurttaşlarının internete erişimini engellemek isteyen ülkeler, bu filtreleri aşmak için gerekli araç ve yöntemleri öneren proxy'leri ve web sitelerini de engellemek için özel bir çaba sarf etmektedir.

İnsan Hakları Evrensel Bildirgesi'nin 19. maddesinde belirtilen 'bilgiye sınırsız erişim güvencesi'ne rağmen, son birkaç yıldır internet sansürüne katılan ülke sayısı çarpıcı bir biçimde artmaya devam etmektedir. İnternet filtreleme uygulaması dünya çapında yaygınlaşırken aktivistler, programcılar ve gönüllüler tarafından yaratılan, uygulanan ve yaygınlaştırılan sansür aşma araçlarına erişim de yaygınlaşıyor.

İnternet sansürünü aşmanın çeşitli yollarını incelemekten önce, bu filtrelerin nasıl çalıştığına ilişkin temel bir kavrayış geliştirmelisiniz. Bunu yaparken, internete bağlanmanın büyük ölçüde basitleştirilmiş modelini göz önünde bulundurmanız yararlı olabilir.

İnternet bağlantınız



Evinizden, ofisinizden, okulunuzdan, kütüphanenizden ve internet kafeden internete bağlanmanızın ilk adımı bir İnternet Servis Sağlayıcısı *ISP* ^[102] aracılığıyla yapılır. *ISP* ^[102], çeşitli internet hizmetlerinin sizi tanınması ve size e-posta ve talep ettiğiniz web sayfaları gibi bilgileri göndermesi için bilgisayarınıza kullanabileceği bir *IP adresi* ^[106] atar. *IP adresinizi* ^[106] öğrenen herhangi biri hangi şehirde olduğunuzu anlayabilir. Bununla beraber, ülkenizdeki belirli bağlantıları olan kuruluşlar bu bilgiyi kesin konumunuzu belirlemek için kullanabilir.

- **ISP'niz**, internete bir modem aracılığıyla erişiyorsanız, hangi binada olduğunuzu ve hangi telefon hattını kullandığınızı bilecektir.
- **İnternet kafemiz, kütüphanemiz ya da iş yeriniz**, verili bir zamanda hangi bilgisayarı kullandığının yanı sıra hangi porttan ya da kablosuz erişim noktasından bağlandığınızı da bilecektir.
- **Devlet organları**, yukarıda belirtilen kuruluşlar üzerindeki nüfuzlarının bir sonucu olarak bu ayrıntıların tümünü biliyor olabilir.

Bu aşamada, *ISP* ^[102]'niz, siz dâhil bütün kullanıcılarını dünyanın geri kalanına bağlamak için ülkenizin ağ altyapısına tabidir. Bağlantınızın diğer ucundaki eriştiğiniz web sitesi ya da internet hizmeti de, kendi ülkesindeki bir *ISP* ^[102] 'den IP adresini alarak, benzer bir süreçten geçer. Tüm teknik ayrıntılar olmaksızın bile bunun gibi bir temel model, filtreleri aşmanızı ve internette anonim kalmanızı sağlayan çeşitli araçları ele alırken yardımcı olabilir.

Web siteleri nasıl engellenir

Esasında, bir web sayfasını ziyaret ettiğinizde, sitenin *IP adresini* ^[106] *ISP* ^[102]'nize göstererek web sunucusunun *ISP* ^[102]'siyle sizi bağlamasını istiyorsunuz. Bu işlem, filtrelenmemiş internet bağlantınız varsa tam olarak bu şekilde gerçekleşir. Ancak, interneti sansürleyen bir ülkedeyken, *ISP* 'niz ilk önce yasaklanmış web sitelerinin *kara listesine* ^[139] bakacak ve ardından da isteğinizi yerine getirip getirmemeye karar verecektir.

Bazı durumlarda, *ISP* ^[102]'lerin kendileri yerine, filtreleme ile uğraşan merkezi bir kurum olabilir. Birçok durumda bir *kara liste* ^[139], *IP adresleri* ^[140] yerine *www.blogger.com* gibi *alan adlarını* ^[141] içerir. Ve bazı ülkelerde filtreleme yazılımları, belirli internet adreslerini engellemeye çalışmak yerine, bağlantınızı izler. Bu tür yazılımlar gönderdiğiniz talepleri ve size dönen sayfaları hassas anahtar sözcüklere bakarak tarar ve ardından da sonuçları görmenize izin verip vermemeye karar verir.

Ve daha da kötüsü, bir web sayfası engellendiğinde bunu bilemeyebilirsiniz bile. Bazı filtreler neden belirli bir sayfanın sansür edildiğini açıklayan engelleme sayfası sağlarken, diğerleri yanıltıcı bir hata mesajı görüntüler. Bu mesajlar, örneğin sayfanın bulunmadığını ya da adresin yanlış yazıldığını ima edebilir.

İnternet sansürü konusunda ülkenizde kullanılan filtreleme teknolojilerinin güçlü ve zayıf yanlarını araştırmaya çalışmak yerine, bir 'en kötü durum bakış açısı' geliştirmek genellikle en kolaydır. Bir başka deyişle şunları varsayabilirsiniz:

- İnternet trafiğinizin anahtar sözcüklerle izlendiğini
- Filtrelemenin doğrudan *ISP* ^[102] düzeyinde uygulandığını
- Engellenen sitelerin hem *IP adresleri* ^[106] hem de *alan adları* ^[135] üzerinden *kara listeye* ^[139] alındığını
- Engellenmiş bir sitenin neden yüklenmediği konusunda size muğlak ya da yanlış yönlendirici bir yanıt verilebileceğini

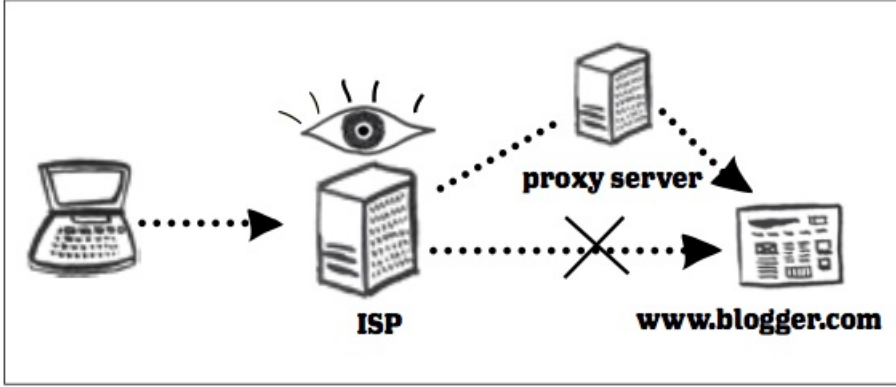
En etkili sansür aşma araçları, hangi filtreleme yönteminin kullanıldığından bağımsız olarak kullanılabilir olduğundan bu karamsar tahminlerde bulunmanın genelde bir zararı olmaz.

Mansour: Bir gün bloğa erişemediğimi ama bir başka ülkedeki arkadaşımın bloğa erişimle ilgili bir sorun yaşamadığını fark edersem bu, web sitesini devletin engellediği anlamına mı gelir?

Magda: Tam olarak öyle değil. Web sitesine sadece buradan erişmek isteyen insanları etkileyen bazı sorunlar olabilir. Ya da bilgisayarında sadece belirli türden web sayfalarına erişirken ortaya çıkan bazı sorunlar olabilir. Bu sorunu test etmek için web sitesini, bir sansür aşma aracıyla ziyaret etmeyi deneyebilirsin. Nihayetinde bu araçların çoğu harici proxy sunucularına bağlıdır ki bu da bir başka ülkedeki bir arkadaşından senin için bir web sitesini sinamasını istemekle aynı işe yarar.

Sansür aşmayı anlamak

Bir web sitesi yukarıda ele alınan yöntemlerden biri kullanılarak engellendiği için doğrudan ziyaret edilemiyorsa, engelin çevresinden dolaşacak bir yol bulmanız gerekecektir. İnterneti filtrelemeyen bir ülkede konuşlanmış güvenli bir [proxy](#) ^[136] sunucusu, istediğiniz web sayfalarını bularak ve onları size ulaştırarak, bu tür bir alternatif yolu size sağlayabilir. [ISP](#) ^[102]'niz açısından siz, internette bir yerlerde bulunan bilinmeyen bir bilgisayarla ([proxy](#) ^[136] sunucusuyla) güvenli bir iletişim kurmuş gibi görüneceksiniz.



Elbette ülkenizde internet sansüründen sorumlu devlet organı (ya da filtreleme yazılımı için güncellemeler sağlayan şirket) eninde sonunda bu 'bilinmeyen bilgisayar'ın gerçekte bir sansür aşma [proxy](#) ^[136]'si olduğunu öğrenecektir. Bu olursa, kullandığınız Proxy'nin [IP adresi](#) ^[106] de [kara listeye](#) ^[139] eklenebilir ve işlemez hale gelir. [Proxy](#) ^[136]'lerin engellenmesi genelde zaman alır, bununla beraber sansür aşma araçlarını yaratanlar ve onları güncelleyenler bu tehdidin farkındadır. Onlar aşağıdaki yöntemlerin birini ya da tümünü kullanarak bu tehditle mücadele ederler:

- **Gizli proxy'lerin** kimliğinin saptanması daha güçtür. Daha az görünür olma eğiliminde olan güvenli [proxy](#) ^[136]'leri kullanmanın önemli olmasının nedenlerinden biri budur. Bununla beraber [şifreleme](#) ^[40], çözümün sadece bir parçasıdır. Bir [proxy](#) ^[136]'nin yöneticileri, gizli kalmak istiyorlarsa, yeni kullanıcılara konumlarını açık ederken bu konuda dikkatli davranmalıdırlar.
- **Tek kullanımlık proxy'ler** engellendikten sonra hızla yenilenebilir. Bu durumda kullanıcılara yenilenen [proxy](#) ^[136]'leri nasıl bulacaklarını bildirmek çok da güvenli olmayabilir. Bunun yerine, bu türden sansür aşma araçları yeni [proxy](#) ^[136]'leri engellenebileceğinden daha hızlı yaygınlaştırmaya çalışır.

Nihai olarak, istediğiniz hizmetleri aramak için güvenilir bir [proxy](#) ^[136]'e eriştiğiniz sürece yapmanız gereken tek şey uygun internet uygulamalarıyla istediğiniz talepleri göndermek ve geri dönen şeylere bakmaktır. Genellikle bu sürecin ayrıntıları bilgisayarınıza kurduğunuz sansür aşma yazılımı tarafından, tarama ayarlarınızı değiştirerek ya da tarayıcınızı web tabanlı bir [proxy](#) ^[136] sayfasına yönlendirerek, otomatik olarak yapılır. Aşağıda ele alınan [Tor](#) ^[111] anonimlik ağı ilk yöntemi kullanır. Ardından da her biri biraz farklı şekilde çalışan temel tek [proxy](#) ^[136] sansür aşma araçları üzerine bir değerlendirme yer alacaktır.

Anonimlik ağları ve temel proxy sunucuları

Anonimlik ağları

Anonimlik ağları, genel olarak, nereden geldiğinizi ve nereye erişmek istediğinizi gizlemek için internet trafiğinizi farklı güvenli [proxy](#) ^[136]'ler arasında 'sektirir'. Bu, web sitelerini ve diğer internet hizmetlerini yüklerken kullandığınız hızı önemli ölçüde azaltır. Bununla beraber [Tor](#) ^[111], [proxy](#) ^[136]'lerinizi ve ziyaret ettiğiniz web sitelerini işleten kişilere güvenmek konusunda endişe etmekten sizi kurtararak, sansür aşmanın güvenilir, emin ve kamusal araçlarını size sağlar. Her zaman olduğu gibi, şifreler ve e-postalar gibi hassas bilgileri bir tarayıcı aracılığıyla değil tokuş etmeden önce, güvenli bir web sitesiyle şifrelenmiş bir bağlantıya, [HTTPS](#) ^[103]'e, sahip olduğunuzdan emin olun.

[Tor](#) ^[111]'u kullanmak için bir yazılım yüklemeniz gerekecektir, bunun sonucunda hem anonimlik hem de sansürü aşmanızı sağlayan bir araca sahip olacaksınız. [Tor](#) ^[111] ağına bağlandığınız her seferinde, üç ayrı güvenli [Tor](#) ^[111] [proxy](#) ^[136]'si

aracılığıyla rastgele bir yol seçersiniz. Bu, bilgisayarınızın IP adresinin [106] ve talepte bulunduğunuz internet servisinin konumunun, ISP [102]'nin ve proxy [136]'lerin kendileri tarafından bilinmemesini güvence altına alır. Bu araç hakkında daha fazla bilgiyi Tor Rehberi'nden öğrenebilirsiniz.

Uygulama: Tor – Dijital Anonimlik ve Sansür Aşma Rehberi [142]

Tor'un güçlü yanlarından biri sadece bir internet tarayıcısıyla değil, çeşitli internet yazılımlarıyla birlikte kullanılabilmesidir. Mozilla Thunderbird [69] dahil e-posta programları, Pidgin [93] dahil farklı mesajlaşma programları Tor aracılığıyla çalışabilir. İster bu hizmetleri kullandığınızı gizlemek için, isterseniz de engellenmiş hizmetlere erişmek için Tor'u kullanabilirsiniz.

Temel sansür aşma proxy'leri

Temel bir sansür aşma proxy [136]'si seçerken göz önünde bulundurmanız gereken üç önemli soru vardır. Birincisi, kullanmayı düşündüğünüz sansür aşma proxy'si web-tabanlı bir araç mı; ayarlarınızı değiştirmenizi mi gerektiriyor; yoksa bilgisayarınıza bir yazılım kurmanızı mı gerektiriyor? İkincisi, güvenli mi? Üçüncüsü, özel mi yoksa kamuya açık mı?

Web-tabanlı proxy ve diğer proxy'ler:

Web-tabanlı proxy [136]'ler belki de kullanımı en kolay olanlardır. Bunlar tarayıcınızı sadece bir proxy [136] web sayfasına yönlendirmenizi, görmek istediğiniz engellenmiş adresi girmenizi ve bir düğmeye tıklamanızı gerektirir. Ardından proxy [136] talep edilen içeriği kendi web sayfası içinde gösterecektir. Her zaman olduğu gibi sayfadaki bağlantıları takip edebilirsiniz ya da farklı bir sayfa görmek istiyorsanız proxy [143]'e yeni bir adres girebilirsiniz. Herhangi bir yazılım yüklemek ya da tarayıcı ayarlarını değiştirmek zorunda değilsiniz, bir başka deyişle web-tabanlı proxy [143]'lerin:

- Kullanımlarının kolay olduğu
- Program kurmanıza ya da ayarları değiştirmenize izin vermeyen internet kafelerdekiler gibi herkese açık bilgisayarlardan erişilebilir oldukları
- Bilgisayarınızda sansür aşma yazılımıyla "yakalanmak"tan endişe duyuyorsanız potansiyel olarak daha güvenli oldukları, söylenebilir.

Web tabanlı proxy [136]'lerin aynı zamanda belirli dezavantajları da vardır. Her zaman sayfaları doğru biçimde göstermezler ve birçok web tabanlı proxy [136], sesli ve görüntülü içerik sunanlar dahil karmaşık web sitelerini yüklemekte başarısız olacaktır. Ayrıca, her ne kadar bütün proxy [136]'ler kullanıcı sayısı arttıkça yavaşlasa da, bu daha çok web tabanlı proxy [136]'lerin sorunu olma eğilimindedir. Elbette web tabanlı proxy [136]'ler sadece web sayfaları için işler. Web tabanlı proxy [136]'ler aracılığıyla engellenmiş bir hizmete erişmek için, örneğin anlık mesajlaşma programını ya da e-posta istemcisini, kullanamazsınız. Son olarak, güvenli web tabanlı proxy [136]'ler sınırlı gizlilik sunar çünkü ziyaret ettiğiniz web sitesinden size dönecek bilgiye erişmek ve onu dönüştürmek zorundadırlar. Bunu yapamazlarsa proxy [136]'den çıkmadan bir linke tıklayamaz ve hedefteki web sayfasıyla doğrudan bir bağlantı kurma teşebbüsünde bulunamazsınız. Bu konu ilerideki kısımda daha fazla ele alınacaktır.

Proxy [136]'lerin diğer türleri genellikle bir program kurmanızı ya da tarayıcınızı veya işletim sisteminizi harici bir proxy [136] adresine göre düzenlemenizi gerektirir. Birinci durumda, sansür aşma programınız, tarayıcınıza proxy [136]'i kullanıp kullanmamasını söyleyen aracı açmanın ve kapamanın bazı yollarını sunar. Bu tür yazılımlar, yukarıda ele alındığı gibi proxy [136]'lerden biri engellendiğinde otomatik olarak onları değiştirmenize izin verir. Tarayıcınızı ya da işletim sisteminizi harici bir proxy [136] adresine göre düzenlemeniz gerekiyorsa, bu proxy [136] engellenirse ya da kullanılamaz hale gelinceye kadar yavaşlarsa değişebilecek olan doğru proxy [136] adresini öğrenmeniz gerekecektir.

Bir web-tabanlı proxy [136]'e göre kullanımı her ne kadar biraz daha zor olsa da sansür aşmanın bu yönteminin karmaşık sayfaları doğru olarak sergilemesi daha olasıdır ve verili bir proxy [136] sunucusunu daha fazla kişi kullanmaya başladığında proxy [136]'nin yavaşlaması daha uzun bir süre alabilir. Dahası bir dizi farklı internet uygulaması için farklı proxy [136]'ler mevcuttur. Örnek verecek olursak, engellenmekten kaçınmak için tüm internet trafiğinizi yeniden yönlendirebilen, tarayıcılar için HTTP proxy [136]'leri, e-postalar için SOCKS proxy [136]'leri, chat programları için VPN proxy [136]'leri bulunmaktadır.

Güvenli ve güvensiz proxyler:

Bu bölümde, güvenli proxy [136] olarak ele aldığımız proxy'den kasıt, kullanıcılarından şifrelenmiş [40] bağlantıları kabul eden bütün proxy [136]'lerdir. Güvensiz bir proxy [136] engellemenin birçok türünü aşmanıza izin verecektir ama bu proxy'ler internet bağlantınız anahtar sözcükler için ya da belirli websitesi adresleri için tarandığında güvenlik açısından başarısız kalacaktır. Güvensiz bir proxy [136]'i normalde şifrelenmiş [40] e-posta hesapları ya da bankacılık web siteleri gibi sitelere erişmek için kullanmak özellikle kötü bir fikirdir. Bunu yaparak normalde gizli olan hassas bilgileri açığa çıkarabilirsiniz. Daha önce de belirtildiği gibi, güvensiz proxy [136]'ler internet engelleme yazılımlarını ve politikalarını güncelleyenler için keşfetmesi ve engellemesi çoğu zaman en kolay olanlardır. Sonuç olarak, ücretsiz, hızlı ve güvenli proxy [136]'lerin var olması, güvenli olmayanları kullanmanız için çok az iyi nedenin olduğu anlamına gelir.

Bir web-tabanlı proxy'nin güvenli olduğunu, proxy [136] web sayfasının kendisine bir HTTPS [144] adresini kullanarak erişebildiğinizde anlarsınız. Webmail hizmetlerinde olduğu gibi, güvenli ve güvensiz bağlantılar desteklenebilir, bu nedenle güvenli adresleri kullandığınızdan emin olun. Bu tür durumlarda, tarayıcınızdan sık sık devam etmek için bir 'güvenlik sertifikası uyarısı'ni kabul etmek zorunda kalacaksınız. Bu, aşağıda ele alınan Psiphon2 [145] ve Peacefire [146] proxy [136]'leri için de geçerli olan bir durumdur. Bu tür uyarılar size, ISP'nizin ya da bir hacker'ın, proxy [136]'e olan bağlantınızı izliyor olabileceğini anlatır. Bu uyarılara rağmen, olanaklı olduğu tüm durumlarda güvenli proxy [136]'leri kullanmak hâlâ iyi bir fikirdir. Bununla beraber, sansürü aşmak için bu tür proxy [136]'lere başvururken, proxy [136]'nin SSL [103]

parmak izini doğrulamadan güvenli web sitelerini ziyaret etmekten, şifreleri girmekten ya da hassas bilgileri paylaşmaktan kaçınmalısınız. Bunu yapmak için [proxy](#) ^[136]'nin yöneticisiyle iletişime geçmenin bir yoluna ihtiyacınız olacak.

Bir web-tabanlı [proxy](#) ^[136]'i işleten kişiye güvenmiyorsanız, bu [proxy](#) ^[136] aracılığıyla hassas bilgilere erişmekten kaçınmalısınız. Bu, [proxy](#) ^[136]'i ziyaret ederken bir güvenlik sertifikası uyarısı görüp görmemenizden bağımsız olarak her zaman geçerlidir. Hatta bu, [proxy](#) ^[136] operatörünü, tarayıcınızı uyarıyı kabul etmesi için yönlendirmeden önce sunucunun parmak izini doğrulayacak kadar iyi tanıyor olsanız bile geçerlidir. Sansürü aşmak için sadece bir [proxy](#) ^[136] sunucusuna bağlıysanız, bu [proxy](#) ^[136] sunucusunun yöneticisi daima sizin [IP adresinizi](#) ^[106] ve hangi web sitelerine eriştiğinizi bilecektir. Bununla beraber daha da önemlisi, eğer bu [proxy](#) ^[136] web-tabanlıysa kötü niyetli bir operatör, webmail'inizin içeriği ve şifreniz dahil, tarayıcınızla ziyaret ettiğiniz web siteleri arasındaki tüm bilgi akışına erişim elde edebilir.

Web-tabanlı olmayan [proxy](#) ^[136]'ler için güvenli bağlantıların desteklenip desteklenmediğini belirlemek için küçük bir araştırma yapmanız gerekebilir. Bu bölümde önerilen [proxy](#) ^[136]'lerin ve anonimlik ağlarının tümü güvenlidir.

Özel proxy'ler ve açık proxy'ler:

Açık [proxy](#) ^[136]'ler herkesten gelen bağlantı taleplerini kabul ederken, özel [proxy](#) ^[136]'ler genellikle bir kullanıcı adı ve parola gerektirir. Açık [proxy](#) ^[136]'lerin kolayca erişilebilir olmak gibi aşikâr bir avantajı olsa da, bu [proxy](#) ^[136]'ler herkes tarafından bulunabileceğinden, çok hızlı bir şekilde aşırı kalabalık olmaya eğilimlidirler. Sonuçta, her ne kadar açık [proxy](#) ^[136]'ler özel olanlar kadar iyi ve teknik olarak gelişmiş olsalar da çoğu zaman görece yavaşlardır. Son olarak, özel [proxy](#) ^[136]'ler kâr amaçlı şirketlerce ya da kişisel veya sosyal olarak tanıdıkları kullanıcılara hesaplar oluşturan yöneticilerce işletilmektedir. Bu nedenledir ki özel bir [proxy](#) ^[136]'i işletenlerin amacını belirlemek genelde daha kolaydır. Ancak özel [proxy](#) ^[136]'lerin bu nedenle daha güvenilir olduğunu varsaymamalısınız. Ne de olsa geçmişte pek çok kez çevrimiçi hizmetler, kâr amacı nedeniyle kullanıcılarını ifşa etmiştir.

Basit, güvensiz, açık [proxy](#) ^[136]'ler genellikle bir arama motorunda 'açık proxy' / 'public proxy' gibi terimleri arayarak bulunabilir. Ama bu şekilde bulunan [proxy](#) ^[136]'lere güvenmemelisiniz. Seçme şansınız varsa, kişisel olarak ya da ismen bildiğiniz ve tanıdığınız, hizmetlerini güvenli olarak sürdürebilecek teknik bilgiye sahip insanlarca işletilen özel, güvenli bir [proxy](#) ^[136]'i kullanmak daha iyidir. Web tabanlı bir [proxy](#) ^[136] kullanıp kullanmamanız kendi özel gereksinimlerinize ve seçimlerinize bağlıdır. Sansürü aşmak için bir [proxy](#) ^[136] kullandığınız her seferinde, [Firefox](#) ^[13] tarayıcısını kullanmanız ve [Firefox Rehberi](#) ^[14]'nde ele alındığı gibi No Script eklentisini kurmanız iyi bir fikirdir. Böyle yapmak, hem kötü niyetli [proxy](#) ^[136]'lerden hem de [IP adresinizi](#) ^[106] keşfetmeye çalışabilecek web sitelerinden sizi korumaya yardım edebilir. Son olarak, [şifrelenmiş](#) ^[147] bir [proxy](#) ^[136]'nin bile güvenli olmayan bir web sitesini güvenli kılmayacağını göz önünde bulundurun. Hassas bilgileri gönderip almadan önce bir [HTTPS](#) ^[103] bağlantınız olduğundan emin olmalısınız.

Güvenilebilir, kesenize uygun ve ülkenizden erişilebilir olduğunu düşündüğünüz, bir bireyin, kuruluşun ya da şirketin [proxy](#) ^[136] hizmetini bulamazsanız, [Anonimlik ağları](#) başlığı altında ele alınan Tor anonimlik ağını kullanmayı göz önünde bulundurmalısınız.

Belirli sansür aşma proxy'leri

Aşağıda, internet filtrelemesini aşmanıza yardım edebilecek birkaç özgül araç ve [proxy](#) ^[136] bulunmaktadır. Yeni sansür aşma araçları düzenli olarak üretilmekte ve var olanlar sık sık güncellenmektedir; bu konuda daha fazla şey öğrenmek için Security in-a-Box web sitesini ve [Okuma önerileri](#) ^[148] bölümünde bahsi geçen kaynakları ziyaret etmelisiniz.

Sanal Özel Ağ (VPN) tabanlı proxy'ler

Aşağıda listesi verilen VPN proxy'leri, "bağlı" olduğunuz sürece tüm internet bağlantınızı proxy'den geçirir. Bu, ülkenizde engellenen e-posta ve anlık mesaj sağlayıcılarını kullanıyorsanız size yardımcı olabilir.

Riseup VPN. Riseup sunucusunda e-posta hesabı olan kullanıcılar içindir. Bu kolektif, güvenli, özel, ücretsiz VPN proxy sunucusuna bağlanma olanağı sunmaktadır. Lütfen [Riseup VPN](#) ^[149] ve [ona nasıl bağlanılır](#) ^[150] konusunda daha fazlasını okuyun.

Hotspot Shield kamuya açık, güvenli, ücretsiz, VPN sansür aşma proxy'sidir. Bunu kullanabilmek için [aracı indir](#) ^[151] meniz ve çalıştırmanız gerekmektedir. Hotspot Shield'ı geliştiren firma reklamlardan gelir elde etmektedir; bu nedenle [şifreleme](#) ^[40] sağlamayan web sitelerini ziyaret etmek için onu kullanırken, tarayıcı pencerenizin en tepesinde "banner reklamı" göreceksiniz. Her ne kadar kanıtlaması olanaksızsa da bu firma, aracı kullananların [IP adreslerini](#) ^[106] depolamak ya da reklam verenlere göndermek yerine, sildiğini iddia etmektedir. **

Your-Freedom güvenli, özel, VPN/SOCKS sansür aşma [proxy](#) ^[136]'sidir . Bir ücretsiz sansür aşma servisine bağlanmak için kullanılacak [ücretsiz bir yazılımdır](#) ^[8] . Bant genişliği ve kullanım süresi üzerinde sınırlama (günde 3 saat, haftada 9 saate kadar) bulunmaktadır. Ücret ödeyerek daha hızlı ve daha az sınırlı olan bir ticarî hizmete erişim de mümkündür. Your-Freedom'ı kullanmak için, [aracı indirmeniz](#) ^[152] ve bir [hesap oluşturma](#) ^[153] gerekmektedir. Her ikisi de [Your-Freedom web sitesinde](#) ^[154] yapılabilir. Ayrıca tarayıcınızı internete bağlanırken [OpenVPN](#) ^[155] proxy kullanacak şekilde düzenlemeniz gerekecektir. Daha fazlasını [Your-Freedom dokümantasyonunda okuyabilirsiniz](#) ^[156].

Freegate açık, güvenli, VPN, ücretsiz yazılım sansür aşma proxy'sidir. [Freegate'in en son sürümünü indirebilir](#) ^[157] ya da Freegate hakkında [ilginç bir makaleyi okuyabilirsiniz](#) ^[158].

SecurityKISS açık, güvenli, VPN, ücretsiz yazılım sansür aşma proxy'sidir. Bunu kullanabilmek için [ücretsiz bir programı indirmeniz ve çalıştırmanız](#) ^[159] gerekmektedir. Bir hesap için kaydolmaya gerek yoktur. Ücretsiz kullanıcılar günlük 300

MB'lık proxy üzerinden internet trafiğiyle sınırlandırılmıştır. Ücretli kullanıcılar için sınırlama yoktur ve kullanabilecekleri daha fazla VPN sunucusu bulunmaktadır. [Daha fazlasını öğrenmek için SecureKISS'in ana sayfasına](#) ^[160] bakınız.

Psiphon3 internet içeriğine sansürsüz erişim sağlamanız için VPN, SSH ve HTTP Proxy teknolojilerinden yararlanan güvenli, kamuya açık bir araçtır. Kullanabilmek için programı [Psiphon3'ün ana sayfasından](#) ^[161] indirmeniz ve hangi modda [VPN, SSH, SSH+] kullanmak istediğinizi seçmeniz gerekir. Phiphone3 Android cihazlarla da birlikte çalışmaktadır. Daha fazlasını öğrenmek için lütfen [ana sayfasına](#) ^[161] bakınız.

Web Proxy'leri:

Peacefire çok sayıda açık, web tabanlı [proxy](#) ^[136]'i destekler. Bu [proxy](#) ^[136]'ler, onlara nasıl eriştiğinize bağlı olarak güvenli ya da güvensiz olabilir. Bir [Peacefire](#) ^[146] [proxy](#) ^[136] kullanırken, siz ve proxy arasında güvenli bir bağlantıya sahip olmak için [HTTPS](#) ^[103] adresi girmelisiniz. Yeni [proxy](#) ^[136]'ler düzenli olarak geniş bir e-posta listesine ilan edilmektedir. Güncellemeleri almak için bu e-posta listesine [Peacefire web sitesi](#) ^[162]'nden kayıt olabilirsiniz.

Okuma önerileri

- [Digital Security and Privacy Manual for Human Rights Defenders](#) ^[25] kitabının 2.5 *Internet Surveillance and Monitoring* ve 2.6 *Censorship circumvention* bölümlerine bakınız.
- FLOSS El kitapları web sitesi [Internet Sansürü Nasıl Aşılır](#) ^[163] üzerine bir rehber içerir.
- Freerk tarafından yazılan [Internet Censorship Wiki](#) ^[164] İngilizce, Almanca ve İspanyolca okunabilir.
- CitizenLab'in [Everyone's guide to by-passing Internet Censorship](#) ^[165] isimli rehberi şu anda İngilizce, Fransızca, Rusça, İspanyolca, Burmaca ve Urdu dillerine çevrilmiştir.
- Reporters Without Borders'in ikinci baskısını yayınladığı [Handbook for Bloggers and Cyberdissidents](#) ^[166] isimli el kitabı Arapça, Burmaca, Çince, İngilizce, Farsça, Fransızca, Rusça ve İspanyolca okunabilir.
- Global Voices Online'dan Ethan Zuckerman, [Anonymous Blogging with Wordpress and Tor](#) ^[167] isimli faydalı bir rehber yayınladı.

9. Sosyal ağ sitelerini kullanırken kendinizi ve verilerinizi nasıl korursunuz

Çevrimiçi topluluklar internetin icadından bu yana var olmuştur. İlk başta dünyanın her yerindeki insanlara belirli konularda iletişim kurma ve bilgi paylaşma olanağı sunan ilan panoları ve e-posta listeleri vardı. Günümüzde sosyal ağ siteleri mesaj, fotoğraf, dosya ve ne yaptığınız ve nerede olduğunuz konusunda son dakika bilgilerini bile paylaşmanıza izin vererek, olası karşılıklı etkileşimin sınırlarını büyük ölçüde genişletti. Bu işlevler yeni ve benzersiz değildir – bu eylemlerin herhangi biri sosyal ağ sitelerine katılmadan internet aracılığıyla gerçekleştirilebilir.

Her ne kadar bu ağlar çok yararlı olabilse de ve çevrimiçi ve çevrimdışı sosyal karşılıklı etkileşimi teşvik etse de, sosyal ağları kullanırken bilgilerinizi kötüye kullanmak isteyen insanlara bilgilerinizi erişilebilir kılıyor olabilirsiniz. Bir sosyal ağ sitesini büyük bir parti olarak düşünün. Orada tanıdığınız insanların yanı sıra hiç tanımadığınız insanlar da vardır. Partinin bir ucundan diğerine, tüm kişisel bilgilerinizin ve o anda ne düşündüğünüzün üzerinde yazılı olduğu sırtınıza asılmış büyük bir tabelayla yürüdüğünüzü hayal edin. Öyle ki herkes, siz farkında olmadan bu tabelayı okuyabilsin. Herkesin sizin hakkınızdaki her şeyi bilmesini gerçekten ister misiniz?

Sosyal ağ sitelerinin özel şirketlere ait olduğunu ve paralarını kişiler hakkında veri toplayarak ve bu verileri özellikle reklamcılara satarak kazandıklarını hatırlayın. Bir sosyal ağ sitesine girdiğinizde internetin özgürlüklerini geride bırakır ve sitenin sahipleri tarafından yönetilen ve düzenlenen bir ağa girersiniz. Gizlilik ayarları, sizi sadece sosyal ağın diğer üyelerine karşı korumayı amaçlar ama verilerinizi şirketin sahiplerine karşı korumaz. Sosyal ağları kullanarak esasında yaptığınız şey, tüm verilerinizi bu şirketlerin sahiplerine vermek ve bu konuda onlara güvenmek anlamına gelir.

Hassas bilgiler ve konular üzerinde çalışıyor; aynı zamanda sosyal ağ hizmetlerini kullanmak istiyorsanız, sosyal ağların yarattığı gizlilik ve güvenlik sorunlarının son derece farkında olmanız önemlidir. İnsan hakları savunucuları, sosyal ağ sitelerinin tehlikelerine karşı özellikle uyarılır ve kendileri VE birlikte çalıştıkları insanlar hakkında ortaya koydukları bilgiler konusunda aşırı derecede dikkatli olmalıdırlar.

Herhangi bir sosyal ağ sitesi kullanmadan önce bu sitelerin sizi nasıl tehlikeye açık kıldığını anlamanız ve ardından da kendinizi ve birlikte çalıştığınız insanları korumak için adımlar atmanız önemlidir. Bu rehber, sosyal ağ siteleri kullanmanın oluşturduğu güvenlik sorunlarını anlamanıza yardım edecektir.

Arka plan senaryosu

Mansour ve Magda kuzey Afrika'da yaşayan insan hakları savunucularıdır. Büyük bir kentin ortasında gerçekleştirilecek bir yürüyüş örgütlemektedirler. Etkinliği yaygınlaştırmak için Facebook'u kullanmak isterler. Ancak yetkililere tüyo vermekten ve ilgi gösteren herkesin izinin sürülmesinden endişe duymaktadırlar. Yürüyüş sırasında yürüyüşün ilerleyişi hakkında bilgi vermek için Twitter'ı kullanmayı planlarlar. Ama ya polis tweet'leri izlerse ve yürüyüşçüleri durdurmak için ekip gönderirse? Mansour ve Magda yürüyüşün fotoğraflarını ve videolarını insanların kimliklerini açığa vurmadan nasıl paylaşacaklarını planlarlar çünkü katılımcıların yargıyla yüz yüze gelmelerinden endişe etmektedirler.

Sizi sosyal ağ araçlarının kullanımını tamamen bırakmaya teşvik etmiyoruz. Bununla beraber, kendinizi ve başkalarını

tehlikeye sokmadan bu araçları kullanabilmeniz için uygun güvenlik önlemleri almalısınız.

Bu bölümden ne öğrenebilirsiniz

- Sosyal ağ sitelerinin, kasıtlı olmaksızın, hassas bilgilerin açığa çıkmasını nasıl kolaylaştırdığını
- Sosyal ağ sitelerini kullanırken, kendiniz ve başkaları hakkındaki bilgileri nasıl güvence altına alacağınızı

Sosyal ağ sitelerini kullanmakla ilgili genel ipuçları

- **Şu soruları daima sorun:**
 - İnternete koyduğum bilgilere kimler erişebilir?
 - Sosyal ağ sitelerine koyduğum bilgileri kim denetliyor ve bu sitelerin sahipleri kim?
 - Bağlantılı olduğum kişiler diğer insanlara benim hakkımdaki hangi bilgileri aktarıyor?
 - Bağlantılı olduğum kişiler, onlar hakkındaki bilgileri diğer insanlarla paylaşmamda bir sakınca görür mü?
 - Bağlantılı olduğum herkese güveniyor muyum?
- Sosyal ağlara erişmek için **güvenli şifreler** kullandığınızdan daima emin olun. Bir başkası sizin hesabınıza girdiyse, sizin hakkınızda ve sosyal ağ aracılığıyla bağlantılı olduğunuz diğer herkes hakkında birçok bilgiye erişim elde ediyordur. Düzenli aralıklarla şifrenizi değiştirin. Daha fazla bilgi için [Güvenli şifreler nasıl oluşturulur ve muhafaza edilir](#) ^[37] başlıklı [3. Bölüm](#) ^[37]'e bakınız.
- Sosyal ağ sitesi tarafından sunulan öntanımlı **gizlilik ayarlarını** ve onları nasıl değiştireceğinizi anladığınızdan emin olun.
- Farklı kampanyalar ve etkinlikler için **ayrı hesaplar/kimlikler** ya da belki de farklı takma adlar kullanmayı düşünün. Unutmayın, bir ağı güvenli olarak kullanmanın anahtarı, o ağın üyelerine güvenmektir. Farklı hesaplara sahip olmak bu tür bir güvenin olanaklı olduğunu garantiye almanın iyi bir yolu olabilir.
- Kamuya açık internet alanlarından sosyal ağ hesabınıza erişirken dikkatli olun. Herkese açık bir makinede tarayıcı kullanırken **şifrenizi ve tarama geçmişinizi** silin. [Hassas bilgiler nasıl yok edilir](#) ^[37] başlıklı [6. Bölüm](#) ^[37]'e bakınız.
- Kullanıcı adınızı, şifrenizi ve gönderdiğiniz diğer bilgileri korumak için **https:// kullanarak sosyal ağ sitelerine erişin**. [http:// yerine https:// kullanmak tarayıcınız ile sosyal ağ siteniz arasındaki trafiği şifreleyerek bir başka güvenlik tabakası ekler](#). Bakınız: [İnternette nasıl anonim kalınır ve internet sansürü nasıl aşılır](#) ^[110] başlıklı [8. Bölüm](#) ^[110].
- Ağınızdaki insanlara güvenseniz bile, **durum güncellemelerinize** çok fazla bilgi koymak konusunda dikkatli olun. Bilgilerinizin bir başkası tarafından kopyalanması kolaydır.
- Sosyal ağların çoğu, diğer sosyal ağlardaki bilgilerinizi birleştirmenize izin verir. Örneğin Twitter hesabınıza bir güncelleme gönderebilirsiniz ve onun aynı zamanda Facebook hesabınızdan da otomatik olarak gönderilmesini sağlayabilirsiniz. **Sosyal ağ hesaplarınızı birleştirirken özellikle dikkatli olun!** Bir sitede anonim olabilirsiniz ama bir başkasını kullanırken kendinizi ifşa edebilirsiniz.
- Bir sosyal ağ sitesindeki içeriğinizin ne kadar güvende olduğu konusunda tedbirli olun. **İçeriğinizin ya da bilgilerinizin birincil saklama yeri olarak bir sosyal ağ sitesine asla bel bağlamayın**. Hükümetlerin bir sosyal ağ sitesinin içeriğini aniden sakıncalı bulmaları durumunda ülke sınırları içinde ona erişimi engellemeleri çok kolaydır. Bir sosyal ağ sitesinin yöneticileri, belirli bir ülkede sansürle yüzleşmektense, sakıncalı içeriği ortadan kaldırmaya karar verebilir.

Kişisel bilgilerinizi göndermek

Sosyal ağ siteleri diğer kullanıcıların sizi bulmasını ve size bağlanmasını kolaylaştırmak için sizin hakkınızda birçok bilgiyi size sorar. Bunun bu sitelerin kullanıcıları için yarattığı belki de en büyük tehlike, gitgide artan bir biçimde yaygınlaşan kimlik sahtekârlığı olasılığıdır. Dahası, çevrimiçi olarak kendiniz hakkında ne kadar çok bilgi verirsiniz, yetkililerin kimliğinizi saptaması ve etkinliklerinizi izlemesi de o kadar kolay olur. Bazı ülkelerin diasporasındaki aktivistlerin çevrimiçi etkinlikleri, yetkililerin, aktivistlerin ana vatanlarındaki aile üyelerini hedef almasına neden olmuştur.

Kendinize sorun: şu bilgileri çevrimiçi post etmeniz gerekli mi?

- doğum tarihleri
- telefon numaraları
- adresler
- aile üyelerinin ayrıntıları
- cinsel yönelim bilgileri
- eğitim ve iş geçmişi

Arkadaşlar, takipçiler ve bağlantılı olduğunuz kişiler

Herhangi bir sosyal ağ uygulamasında kişisel ayrıntılarınızı doldurduktan sonra yapacağınız ilk şey diğer insanlarla

bağlantılar kurmaktır. Varsayımsal olarak, bu bağlantıda olduğunuz kişiler tanıdığınız ve güvendiğiniz kişilerdir –ya da daha önce hiç karşılaşmadığınız ama benzer bir kafa yapısına sahip olduğunuzu düşündüğünüz bir topluluğun sosyal ağına da bağlanmış olabilirsiniz. Anlamanız gereken en önemli şey, bu çevrimiçi topluluğun hangi bilgilerinize sahip olmasına izin verdiğinizdir.

Sizin hakkınızda birçok bilgiyi elinde bulunduran Facebook gibi bir sosyal ağ hesabı kullanırken, sadece tanıdığınız ve gönderdiğiniz bilgileri kötüye kullanmayacağı konusunda güvendiğiniz kişilerle bağlantı kurmayı düşünün.

Durum güncellemeleri

Twitter’da, Facebook’da ve benzer ağlarda durum güncellemeleri şu soruları yanıtlar: Şimdi ne yapıyorum? Ne oluyor? Durum güncellemeleri hakkında anlamanız gereken en önemli şey, bunları gerçekten kimlerin görebileceğidir. Sosyal ağ uygulamalarının bir çoğunda, durum güncellemelerinin öntanımlı ayarları, internetteki herkesin güncellemelerinizi görebileceği şekilde ayarlanmıştır. Bu güncellemeleri sadece bağlantılı olduğunuz kişilerin görmesini istiyorsanız, sosyal ağ uygulamasına güncellemelerinizi herkesten gizli tutmasını söylemeniz gerekir.

Twitter’da bunu yapmak için “Tweet’lerimi Korum” seçeneğini arayın. Facebook ayarlarınızı güncellemelerinizi “Sadece Arkadaşlar” ile paylaşacak şekilde değiştirin. Bu ayarlara geçerseniz bile bilgilerinizin takipçileriniz ve arkadaşlarınız tarafından yeniden gönderilmesinin ne kadar kolay olduğunu göz önünde bulundurun. Ağdaki arkadaşlarınızla, sosyal ağ hesaplarınıza gönderilen bilginin aktarılması konusunda ortak bir yaklaşım üzerinde anlaşın. Arkadaşlarınızın diğer insanların bilmesini istemeyebileceği hangi bilgileri açığa çıkardığınız konusunda da düşünmelisiniz; bu konuda hassas olmanız ve diğerlerinin de sizin bilgilerinizi ortaya koyarken hassas davranmalarını onlardan istemeniz önemlidir.

Durum güncellemelerindeki bilgilerin kişiler aleyhine kullanıldığı birçok olay bulunmaktadır. ABD’de öğretmenler, öğrencileri hakkında ne hissettikleri üzerine güncellemeler gönderdikten sonra işten çıkarıldı; diğer çalışanlar işverenleri hakkında güncellemeler gönderdikleri için işlerini yitirdi. Bu neredeyse herkesin dikkatli olması gereken bir konudur.

İnternet içeriği paylaşmak

Bir web sitesinin bağlantısını paylaşmak ve arkadaşlarınızın dikkatini çekmek kolaydır. Ama başka kimler dikkat ediyor ve tepkileri ne olacak? Baskıcı bir rejimi yıkmayla bir şekilde ilişkili bir siteyi beğendiğinizi söylüyorsanız bu rejim sizinle ilgilenabilir ve sizi hedef alabilir.

Paylaştığınız ya da ilginç olarak işaretlediğiniz şeyleri görenlerin sadece bağlantılı olduğunuz kişiler olmasını istiyorsanız gizlilik ayarlarınızı kontrol ettiğinizden emin olun.

Konumunuzu ifşa etmek

Sosyal ağ sitelerinin birçoğu konum bilgileriniz erişilebilirse onları görünür kılacaktır. Bu işlev genellikle GPS’i açık telefonlarla sosyal ağ ile etkileşimde bulunduğunuzda sağlanır ama cep telefonundan bağlanmadığınız zamanlarda bunun olasılık dışı olduğunu varsaymayın. Bilgisayarınızın bağlandığı ağ da konum bilgisi sağlıyor olabilir. En emniyetlisi ayarlarınızı iki kez kontrol etmenizdir.

Fotoğraf ve video paylaşım sitelerindeki konum ayarlarına özellikle dikkat edin. Bu sitelerin konum bilgilerinizi paylaşmadıklarını varsaymayın: Emin olmak için ayarlarınızı iki kez kontrol edin.

Ayrıca, Electronic Frontier Foundation’ın web sitesinden [On Location Privacy, and How to Avoid Losing it Forever](#) ^[168] başlıklı metne bakınız.

Video/fotoğraf paylaşmak

Fotoğraflar ve videolar insanların kimliklerini kolayca açığa çıkarır. Paylaşımında bulunmadan önce, fotoğrafını ya da videosunu gönderdiğiniz kişilerden izin almanız önemlidir. Bir başkasının görüntüsünü gönderiyorsanız onların mahremiyetinden nasıl ödün verdiğinizin farkında olun. Rızasını almadan hiç kimsenin fotoğrafını ya da videosunu hiçbir zaman göndermeyin.

Fotoğraflar ve videolar kasıtsız olarak birçok bilgiyi de açığa çıkarır. Birçok fotoğraf makinesi, fotoğrafa fotoğrafın tarihini, zamanını, konumunu ve fotoğraf makinesinin tipini vb. açığa çıkaran gizlenmiş veriler (meta etiketleri) yerleştirir. Fotoğraf ve video paylaşım siteleri, bu sitelere içerik yüklediğinizde bu bilgileri yayınlatabilir.

Anlık sohbet

Sosyal ağ sitelerinin birçoğu arkadaşlarınızla gerçek zamanlı olarak görüşmeler yapmanıza izin veren araçlara sahiptir. Bu araçlar Anlık Mesajlaşma gibi çalışır ve hem kiminle iletişim kurduğunuzu hem de ne üzerine iletişim kurduğunuzu ifşa edebileceğinden internetteki en güvensiz iletişim kurma yollarından biridir.

Https ile web sitesine bağlanmak güvenli çevrimiçi sohbet için asgari bir gerekliliktir ancak bu bile sohbet programınızın güvenli bir bağlantı kullandığına dair yeterli bir garanti değildir. Örneğin Facebook sohbet HTTPS’den farklı bir kanal kullanır (ve bilgileri ifşa etmeye çok daha fazla eğilimlidir).

Çevrimiçi sohbet için şifreleme kullanan uygulamaları kullanmanız daha güvenlidir. Örneğin, Pidgin uygulamasını Off-the-record (kayıt dışı) eklentisiyle birlikte kullanabilirsiniz. 'Pidgin – güvenli anlık mesajlaşma' uygulama rehberini okuyunuz.

Grup, etkinlik ve topluluklar oluşturmak ve onlara katılmak

Bir gruba ya da topluluğa katıldığınızda insanlara hangi bilgileri veriyorsunuz? Bu bilgiler sizin hakkınızda ne söylüyor? Öte yandan, insanlar sizin oluşturduğunuz bir gruba veya topluluğa katıldıklarında dünyaya ne ilan ediyorlar? İnsanları nasıl riske sokuyorsunuz?

Çevrimiçi bir gruba ya da topluluğa katıldığınızda hakkınızdaki bazı şeyleri başkalarına görünür kılmış olursunuz. Örneğin belirli bir siyasi grubun çevrimiçi sosyal ağlarından birini takip ediyorsunuz, insanlar bu grubun söylediklerini ya da yaptıklarını desteklediğinizi ya da grupla aynı fikirde olduğunuzu varsayabilir. Bu da sizi risk altına sokabilir. Ayrıca tanımadığınız çok sayıda üyesi olan bir gruba katılmanız, hesabınıza uyguladığınız gizlilik ya da güvenlik ayarlarından ödün verdirebilir. Bu nedenle gruba katılmadan önce hangi bilgilerinizi verdiğinizi düşünün. Yabancıların sizi tanımasını sağlayabilecek gerçek fotoğrafınızı ve adınızı mı kullanıyorsunuz?

Öte yandan, bir grup oluşturduğunuzda ve insanlar ona katılmayı seçtiğinde bunu yaparak dünyaya ne ilan ediyorlar? Örneğin, diyelim insanlara yardım etmek için bir gay ve lezbiyen destek grubu kurdunuz ama bu gruba katılarak insanlar, açıkça gay ya da gay dostu olarak kendilerini tanımlamış olurlar. Bu da gerçek dünyada onları tehlikeye sokabilir.

Uygulama: **Sosyal ağ iletişim araçları: Facebook, Twitter, YouTube ve diğerleri** ^[169] ile uygulamaya başlayın

10. Cep telefonları nasıl olabildiğince güvenli kullanılır

Cep telefonları günlük iletişimimizin ayrılmaz bir parçasıdır. Tüm cep telefonları sesli iletişim ve yazılı mesajlaşma kapasitesine sahiptir. Küçük boyutları, görece düşük fiyatları ve farklı alanlarda kullanılabilir olmaları, bu cihazları iletişim ve örgütlenme amacıyla kullanan hak savunucuları için paha biçilemez kılar.

Daha fazla fonksiyonu olan taşınabilir cihazlar kısa bir süre önce erişilebilir hale geldi. Bu cihazlar, **GPS** ^[170], multimedya kapasitesi (fotoğraf, görüntü ve ses kaydı ve bazen de aktarımı), veri işleme uygulamaları ve internete erişim gibi fonksiyonlar sunabilir. Ancak, taşınabilir ağların işleyiş biçimleri ve altyapısı, internetin işleyişinden temelde farklıdır. Bu, kullanıcıların mahremiyetine ve onların bilgi ve iletişimlerinin bütünlüğüne yönelik ek güvenlik sorunlarını ve riskleri beraberinde getirir.

Cep telefonlarının doğası gereği güvensiz olduğunu kavrayarak işe başlamak önemlidir:

- Cep telefonlarından gönderilen bilgiler saldırılara açıktır.
- Cep telefonlarında depolanan bilgiler saldırılara açıktır.
- Telefonlar bulundukları konum hakkında bilgi vermek için tasarlanmışlardır.

Bu sorunları ve telefonların doğası gereği saldırılara açık olması karşısında bir kullanıcının neler yapabileceğini ele alacağız.

Arka plan senaryosu

Borna ve oğlu Delir fabrika işçileridir ve bir işçi sendikası kurulmasına yardım etmektedirler. Çabaları, yerel hükümetle iyi ilişkiler içinde olan fabrika sahiplerinin direnişiyle karşılaşmaktadır. Borna'nın ustabaşı onu, yönetimin gözetiminde olabileceği ve kiminle konuştuğuna dikkat etmesi gerektiği konusunda uyarıyordu. Borna sendika çalışmaları için bir cep telefonu satın almıştı. Delir yeni cep telefonunu bazı örgütlenme etkinliklerinde güvenli olarak kullanması konusunda babasına yardım etmektedir.

Bu bölümden ne öğrenebilirsiniz

- Cep telefonu ile iletişim kurmak ve veri depolamak neden güvenli değildir
- Cep telefonu kullanmanın güvenliğini arttırmak için hangi adımları atabilirsiniz
- Cep telefonunuz aracılığıyla gözetlenmenizin ya da izinizin sürülmesinin olasılığını nasıl azaltabilirsiniz
- Cep telefonunuzu kullanarak anonim kalma olasılığınızı nasıl arttırabilirsiniz

Taşınabilir cihazlar ve güvenlik

Cep telefonunu kullanırken, kendimizi, ilişkide olduğumuz kişileri ve verilerimizi korumak için, bilgiye dayanan kararlar almamız gerekir. Cep telefonu ağlarının ve altyapısının işleyiş biçimleri, kullanıcıların bilgilerinin ve iletişimlerinin mahremiyetini ve güvenliğini koruma becerilerini önemli ölçüde etkilemektedir.

- Cep telefonları ağları, ticari kurumlar tarafından işletilen özel ağlardır ki bu ticari kurumlar devletin tekelci denetimi altında olabilir. Bu ticari kurumların (ya da devletin) pratikte müşterilerinin bilgilerine ve iletişimlerine sınırsız erişimi vardır; bunun yanı sıra bu kurumlar aramaları dinleme, yazılı mesajları okuma ve her cihazın (ve böylece de onun kullanıcısının) konumunu izleme yeteneğine de sahiptir.

- Taşınabilir cihazların İşletim Sistemleri, çeşitli servis sağlayıcılarının şartnamelerine göre ve bu şirketlerin kendi ağlarında çalışması için, telefon üreticileri tarafından özel olarak tasarlanır ve yapılandırılır. Sonuç olarak, işletim sistemleri herhangi bir aygıtın servis sağlayıcıları tarafından daha iyi izlenebilmesini sağlayan gizli özellikler içerebilir.
- Cep telefonlarında bulunan işlevlerin sayısı son birkaç yılda arttı. Modern cep telefonları aslında, cep telefonu işlevleri olan internet bağlantılı taşınabilir küçük bilgisayarlardır.

İletişiminizin hangi açılardan daha çok korunmaya gereksinim duyduğunu bulmak için, kendinize birkaç soru sormanız yardımcı olabilir: Telefon konuşmalarınızın ve yazılı mesajlarınızın içeriği nedir? Kimlerle ve ne zaman iletişim kuruyorsunuz? Nereden arıyorsunuz? Bilgiler birçok yönden saldırılara açıktır:

- **Bilgiler bir cep telefonundan gönderildiğinde saldırılara açıktır**
Örnek: Her cep telefonu sağlayıcısı kendi ağı kullanılarak gönderilen tüm yazılı ve sesli mesajlara tam erişime sahiptir. Birçok ülkedeki telefon servisleri tüm iletişimin kaydını hukuken tutmak zorundadır. Bazı ülkelerde telefon servisleri devletin tekeli denetimi altındadır. Ayrıca, sesli ve yazılı iletişim, cep telefonunun yakınlarındaki üçüncü kişilerce pahalı olmayan ekipmanlarla gizlice dinlenebilir.
- **Göndericinin ve alıcının telefonlarındaki bilgiler saldırıya açıktır**
Örnek: Cep telefonları her türden veriyi depolayabilir: arama geçmişi, gönderilen ve alınan yazılı mesajlar, adres defteri bilgileri, fotoğraflar, video klipler, metin dosyaları. Bu veriler bağlantıda olduğunuz kişileri, sizin ve meslektaşlarınız hakkındaki kişisel bilgileri ifşa edebilir. Bu bilgileri güvence altına almak güçtür hatta –bazı telefonlarda– imkansızdır. Modern cep telefonları cep boyutunda bilgisayarlardır. Daha fazla özellik daha yüksek riskler getirir. Dahası ,internetle bağlanabilen telefonlar bilgisayarların ve internetin güvenlik açıklarına da tabidir.
- **Telefonlar bulundukları konum hakkında bilgi verir**
Örnek: Her cep telefonu olağan işleyişinin bir parçası olarak, otomatik ve düzenli aralıklarla, telefon servis sağlayıcısını nerede olduğuna dair bilgilendirir. Dahası günümüzde birçok telefon GPS ^[170] işlevlerine sahiptir. Bu kesin konum bilgisi; fotoğraf, SMS ve internet talepleri gibi telefondan gönderilen diğer verilere de yerleştirilmiş olabilir.

Teknolojinin evrimi daha fazla özelliğin yanı sıra daha fazla riski de beraberinde getirdi.

Borna: Oğlum, şu andan itibaren bu cep telefonunu sadece toplantıları planlamak için kullanmaya karar verdim çünkü fabrikadaki telefonu ve hatta evdekini bile dinliyor olabilirler.

Delir: Baba sonunda bir cep telefonuna sahip olman harika, ama telefonunun neler yapıp neler yapamayacağını biliyor musun?

Borna: Tabii ki! Birini arayabilirsin, onlarla konuşursun, onlar da seninle konuşur. Bunu nerede istersen yapabilirsin. VE başkalarına kısa mesajlar gönderebilirim.

Delir: Bunların hepsi doğru ama hepsi bu değil. Bugünlerde bu tür cihazlarla yapabileceğin birçok şey var. Ama bazı risklerden ve güvenlik önlemlerinden söz edelim, özellikle de bazı kişilerin kimlerle görüştüğüne ve neler dediğine ilgilendiğini düşünüyorsan.

İlerleyen bölümler, cep telefonlarını kullanırken ortaya çıkabilecek güvenlikle ilgili tehlikelerin olasılığını düşürmek için atabileceğiniz bir dizi basit adımı ele almaktadır.

Taşınabilirlik ve bilginin tehditlere açık olması

İnsanlar çoğu zaman hassas bilgiler içeren cep telefonları taşırlar. İletişim geçmişi, yazılı ve sesli mesajlar, adres defterleri, ajandalar, fotoğraflar ve diğer yararlı telefon işlevleri, telefon veya veriler kaybolduğunda ya da çalındığında son derece zarar verici olabilir. Cep telefonunuza aktif ve pasif olarak depolanan bilginin farkında olmak yaşamsal öneme sahiptir. Bir telefonda depolanan bilgiler, telefonu kullanan kadar bu telefonun adres defterinde, mesaj kutusunda, fotoğraf albümünde vb. bulunan herkes hakkında bilgi verebilir.

İnternete bağlanan cep telefonları; bu kitabın diğer bölümlerinde ele alındığı gibi, bilgi güvenliği, anonimlik, bilgi kurtarımı, bilgi kaybı ya da hırsızlığı ve bilgilerinize müdahale edilmesi ile ilgili internet ve bilgisayar kullanmanın getirdiği risklere ve zayıflıklara da tabidir.

Kullanıcılar, bu güvenlik risklerinin bazılarını en aza indirmek için, telefonlarının potansiyel güvenlik sorunlarının yanı sıra onun kurulum seçeneklerinin de farkında olmalıdır. Olası sorunların ne olduğunu bildiğinizde önleyici tedbirler alabilirsiniz.

Borna: Cep telefonlarının bir avantajı, toplantılarımızı sokakta yürürken cep telefonu kullanarak organize edersek, bu kişilerin konuşmalarımıza kulak misafiri olamayacak olmaları. Delir: Tehdit unsuru oluşturan bu kişilerin telefon şirketiyle bağlantılı olduklarını mı söylemiştin?

Borna: Evet, bilgi almak için telefon teknisyenlerine rüşvet verdikleri söyleniyor.

Delir: Bu yeni aldığın cep telefonu aboneliği için kendi kimliğine ve adresine kayıt olduysan, konuşmalarının izi sana kadar sürülebilir. Yaptığın her aramanın kaydı, senin aboneliğinin ve kimliğine bağlantılıdır. Kendi kimliğine mi abone oldun?

Borna: Hayır, amcanın dükkânından ikinci el bir telefon aldım; telefonun temiz ve kullanımının güvenli olduğunu söyledi. Telefonuna taktığın ön ödemeli (faturasız) çiplerden satın almama da yardımcı oldu.

Delir: Evet, onlara SIM kart ^[171] deniyor. Telefon şirketleri, telefon numaralarıyla ve SIM kart kimlik numarasıyla VE telefonun kimlik numarasıyla yapılan her aramanın ya da aktarımın izini sürer. Öyle ise, hangi telefon numarasının YA DA telefonun kimlik numarasının YA DA SIM kart kimlik numarasının sana ait olduğunu bilirlerse senin telefon kullanma örüntüne erişebilirler.

Borna: Ve öyle ise, sanırım görüşmelerimi cep telefonumdan bile dinleyebilirler?

Delir: Amcam sayesinde telefonun senin adına kayıtlı değil ve SIM kartın da hiçbir şekilde seninle bağlantılı değil. Şu durumda, SIM kartının ve telefonunun nerede olduğunu izini sürseler bile SIM kartın ve telefonunun seninle bağlantılı olduğunu bilemezler.

-
- [10.2.1 Telefon güvenliği için en iyi pratikler](#) ^[172]
 - [10.2.2 Temel işlevler, takip edilebilirlik ve anonimlik](#) ^[173]
 - [10.2.3 Yazılı iletişim – SMS / Metin mesajları](#) ^[174]
 - [10.2.4 Sesli iletişim ve mesajlaşmanın ötesindeki işlevler](#) ^[175]

Telefon güvenliği için en iyi pratikler

Diğer cihazlarda olduğu gibi cep telefonunuzdaki veri güvenliği için ilk savunma hattı, telefonunuzun ve SIM kartınızın ^[171] ele geçirilmeye ya da hile ile telefonunuzda değişiklik yapılarak kontrol edilmesine karşı fiziksel güvenliğidir.

- Telefonunuzu daima yanınızda bulundurun. Onu sahipsiz bırakmayın. Telefonunuzu umumi yerlerde sergilemekten kaçının.
- Daima telefonunuzun güvenlik kilit kodunu ya da PIN kodlarını kullanın ve bunları sır olarak saklayın. Daima öntanımlı fabrika ayarlarını değiştirerek, bu kodları size özel kılın.
- SIM kartınızı, ek hafıza kartınızı, pili ve telefonu bir işaretle fiziksel olarak ve yabancılar tarafından hemen fark edilmeyecek şekilde işaretleyin (çizin) (küçük bir işaret, karakterler ya da sayılar çizin ya da normal ışıktaki görünmez olan morötesi boya kullanmayı deneyin). Telefonun hareketli parçalarının birleştiği yerlere basılı, taklit edilemez güvenlik etiketleri ya da bant yapıştırın. Bu herhangi bir şeyin değiştirilip değiştirilmediğini kolayca anlamanıza yardımcı olacaktır (örneğin, telefonunuzun hareketli parçaları bir başkası tarafından açılırsa etiket ya da bant yanlış hizalanacak ya da fark edilebilir bir iz bırakacaktır).
- SIM kartınızda, ek hafıza kartınızda ve telefonunuzun hafızasında hangi bilgileri kayıtlı tuttuğunuzun farkında olduğunuzdan emin olun. Hassas bilgileri telefonunuzda depolamayın. Bu tür bilgileri depolamanız gerekiyorsa bunları, gerektiğinde kolayca bir köşeye atılabilecek olan harici bir hafıza kartına kaydetmeyi göz önünde bulundurun –bu tür bilgileri telefonun dahili hafızasına kaydetmeyin.
- SIM kartınızı, (varsa) ek hafıza kartınızı koruyun; bu kartlar iletişim bilgileriniz ve SMS mesajlarınız gibi hassas bilgiler içerir. Örneğin telefonunuzu servise verdiğinizde SIM kartınızı ve ek hafıza kartınızı orada bırakmadığınızdan emin olun.
- Telefonunuzu elden çıkarırken telefonunuzda, SIM ya da hafıza kartında depolanmış herhangi bir bilgiyi de telefonunuzla birlikte vermediğinizden emin olun. Hatta telefonunuz ya da kartlar bozulmuş veya günü geçmiş bile olsa buna dikkat edin. SIM kartlarını tahrip ederek elden çıkarmak belki de en iyi seçenektir. Telefonunuzu birine vermeyi, satmayı ya da yeniden kullanmayı düşünüyorsanız tüm bilgilerin silinmiş olduğundan emin olun.
- Sadece güvenilir telefon satıcılarını ve tamir dükkânlarını kullanmayı düşünün. Bu, ikinci el telefon edinirken ya da telefonunuzu tamir ettirirken bilgilerinizin kötü niyetli ellere geçme ihtimalini azaltır. Yetkili ama rastgele seçilmiş bir telefon satıcısından telefonunuzu almayı düşünün –böylece telefonunuzun, bir casus yazılım kurularak sizin için özel olarak hazırlanmış olması şansını azaltırsınız.
- Telefon bilgilerinizi düzenli olarak bir bilgisayarda yedekleyin. Yedeklemeyi güvenli bir biçimde saklayın (bakınız: [4. Bölüm Bilgisayarınızdaki hassas dosyaları nasıl korursunuz](#) ^[41].) Bu, telefonunuzu kaybettiğinizde verilerinizi yerine koymanızı sağlar. Bir yedeklemeye sahip olmanız (telefonunuz kaybolduğunda ya da çalındığında) hangi bilgilerden ödün verilebileceğini hatırlamanıza yardımcı olur, böylece gerekli adımları atabilirsiniz.
- 15 haneli seri no ya da IMEI numarası (Uluslararası Mobil Cihaz Kodu), telefonunuzu tanımlamaya yardım eder. Bu kod birçok telefonda *#06# tuşlayarak, telefon pilinizin arkasına bakarak ya da telefonun ayarlarına bakarak erişilebilir. Bu kod, çalınması durumunda, telefonunuzun izini sürmeye ve mülkiyetini çabucak kanıtlamaya yardımcı olabileceğinden, bu kodu bir yere not alın ve telefonunuzdan ayrı olarak saklayın.
- Telefonunuzu servis sağlayıcısına kaydettirmenin avantajlarını ve dezavantajlarını düşünün. Telefonunuzun çalındığını bildirdiğinizde servis sağlayıcı, telefonunuzun daha fazla kullanılmasını durdurmalıdır. Ancak kaydetmek, telefon kullanımınızın kimliğinize bağlanması anlamına gelir.

Temel işlevler, takip edilebilirlik ve anonimlik

Telefonunuzla yaptığınız her iletişimde telefonunuz, en yakınınızdaki sinyal kulelerini telefonunuzun varlığı konusunda harekete geçirir. Bu sinyallerin ve iletişimlerin sonucu olarak ağ servis sağlayıcınız cep telefonunuzun kesin coğrafi konumunu her zaman bilir.

Borna: Bu telefon hakkında bilmem gereken başka bir şey var mı?

Delir: Gerçekten seni izlemeye çalıştıklarından şüpheleniyorsan, evet.

Borna: Sanmıyorum ama bunu yapabilirler mi?

Delir: Evet. Telefonun açıksa VE teknisyenin ağ trafiğine erişimi varsa VE sistemdeki hangi telefonun sana ait olduğunu biliyorlarsa bunu yapabilirler.

Borna: Bu olmayacak çünkü oraya gittiğimde telefonumdan arama yapmayacağım.

Delir: Bu bir şeyi değiştirmez baba. Telefonun, şarj edilmiş ve kullanıma hazır olarak senin yanında olduğu sürece, nereye gittiğinin izi sürülecek ve telefonun yakındaki baz istasyonlarıyla haberleşecektir, çünkü telefonun bunu yapmak zorunda. Öyleyse herhangi bir zamanda, senin konumun telefon ağının en yakın kulelerinin arasında bir yerdedir.

Borna: O zaman oraya gidinceye kadar telefonumu kapatmalı mıyım?

Delir: En iyisi onu hiç yanına almaman. Senin için ikinci en iyi şey telefonunu kapalı tutman VE gitmeden önce pilini çıkarman, dönmeden önce de telefonunu açmamandır.

Borna: Ne? Kapatmam yeterli değil mi?

Delir: Güvende olduğundan emin olmak için pili çıkarmalısın çünkü telefon bir aktarım cihazıdır ve piller takılı olduğu sürece, küçük bir ihtimal de olsa, birilerinin senin bilgin olmaksızın bir şekilde telefonunu açması olasıdır.

Anonimlik hakkında

Telefon görüşmelerinizde ya da SMS mesajlarınızda hassas bilgiler paylaşıyorsanız cep telefonlarının yukarıda bahsi geçen iz sürme 'özellikleri'nin farkında olun:

- Her zaman farklı yerlerden arama yapın ve sizinle bağlantılı olmayan konumlar seçin.
- Telefonunuzu pili çıkarılmış olarak kapalı tutun, seçtiğiniz konuma gidin, telefonunuzu açın, görüşmenizi yapın, telefonunuzu kapatıp pilini çıkarın. Arama yaptığınız her seferinde bunu alışkanlık haline getirmeniz, şebekenin hareketlerinizin izini süremeyeceği anlamına gelir.
- Telefonunuzu ve SIM kartınızı ^[171] sık sık değiştirin. Onları arkadaşlarınız ya da ikinci el dükkânlar arasında dolaşıma sokun.
- Bölgenizde mevcutsa, kayıt edilmemiş ön ödemeli SIM kartlar kullanın. Telefon ya da SIM kart için kredi kartıyla ödeme yapmaktan kaçının, böylece kimliğiniz ile telefonunuz ve SIM kartınız arasında bir bağlantı oluşturmamış olursunuz.

Borna: Telefonumun, kapalıymış gibi görünse bile, benim konumum hakkında baz istasyonlarıyla iletişim kurduğunu mu söylüyorsun?

Delir: Evet ama daha kötüsü de var.

Borna: Ne?

Delir: Telefonununa gizlice kurulabilen ve uzaktan telefonunu çalıştırabilen ve senin bilgin olmaksızın bir numarayı arayabilen programlar olduğunu söylüyorlar. Telefonuna böyle bir program kurulmuşsa, toplantınızı başlattığınızda, telefonun bir kayıt ve aktarım cihazı gibi hareket edecektir.

Borna: Hayır! Sahiden mi?

Delir: Teknik olarak bunu yapmak oldukça kolay. Ama telefonunun pili takılı değilse bunların hiçbirisi gerçekleşemez ve böyle bir olasılığa karşı güvende olursun.

Borna: Sanırım çok dikkatli olmak istiyorsam, telefonumu yanıma almayacağım demektir. Acaba hiç mi cep telefonu kullanmasam diye düşünüyorum.

Delir: Lütfen baba. Bana yeni şeylerden korkmamam gerektiğini söyledin. Cep telefonları da böyle, sadece faydalarını ve riskleri bilmen gerekir. Sadece dikkatli ol. Riskleri bilirsen onlardan kaçınmak için önlemler alabilirsin.

Dinlenme hakkında

Telefonunuz sizin bilginiz olmaksızın mikrofonunun menzili içindeki herhangi bir sesi kaydetmek ve aktarmak için

ayarlanabilir. Bazı telefonlar, kapalıymış gibi görünseler bile, uzaktan açılabilir ve bu şekilde harekete geçirilebilir.

- Güvenmediğiniz hiç kimsenin telefonunuza fiziksel olarak erişmesine hiçbir zaman izin vermeyin; bu, telefonunuza casus yazılım kurmanın yaygın bir yoludur.
- Özel ve önemli toplantılar gerçekleştiriyorsanız telefonunuzu kapatın ve pilini çıkarın. Ya da telefonunuzu yanınızda taşımayın, tamamen güvenli olduğunu bildiğiniz bir yerde bırakın.
- İletişim halinde olduğunuz herkesin de burada açıklanan önlemleri uyguladığından emin olun.
- Ek olarak, halka açık yerlerde ya da güvenmediğiniz yerlerde telefonunuzu kullanmanın sizi geleneksel dinleme tekniklerine ya da telefonunuzun çalınma tehlikesine açık kıldığını unutmayın.

Aramalarınıza müdahale edilmesi hakkında

Genellikle, cep telefonu şebekesi üzerinden yapılan sesli iletişimin (ve gönderilen yazılı mesajların) şifrelemesi görece zayıftır. Üçüncü kişilerin, telefonun yakınlarındaysalar ve ondan aktarım alabiliyorlarsa, yazılı iletişiminize müdahale etmek ya da aramalarınızı dinlemek için kullanabileceği ucuz teknikler bulunmaktadır. Elbette cep telefonu sağlayıcılarının tüm sesli ve yazılı haberleşmelerinize erişimi vardır. Görüşmelerinizi, cep telefonu sağlayıcılarının gizlice dinleyemeyeceği şekilde şifrelemek, şu aşamada, pahalı ve/ya da teknik olarak külfetlidir – bununla beraber, bu araçların yakın zamanda ucuzlaması beklenmektedir. Şifrelemeyi devreye sokmak için telefonunuza ve iletişim kurmak istediğiniz kişinin telefonuna şifreleme uygulaması kurmanız gerekir. Ardından bu uygulamayı şifrelenmiş aramalar ve/ya da mesajlar almak ve göndermek için kullanabilirsiniz. Mevcut şifreleme programları 'akıllı' olarak adlandırılan telefonların sadece birkaç modeli tarafından desteklenmektedir.

Skype ve cep telefonları arasındaki iletişim de, -sinyal bir noktada şifrelenmenin olmadığı mobil şebekeye geçeceğiinden-, şifreli değildir.

Yazılı iletişim – SMS / Metin mesajları

Hassas bilgilerinizin güvenle aktarımı için yazılı mesaj servislerine güvenmemeniz gerekir. Değiş tokuş edilen mesajlar düz metin olarak yazıldığından güvenli ve gizli aktarım için uygun değildir.

Borna: Cep telefonumla hiçbir zaman konuşma yapmasam, sadece küçük mesajlar alıp versem ne olur? Konuşma yoksa onlar da dinleyemez ve mesajlaşma da oldukça hızlı, değil mi?

Delir: Bir dakika. Bu mesajlara müdahale etmek kolaydır ve şebekede düz metin olarak dolaşıp duran ve bir kuleden diğerine aktarılırken kaydedilen bu mesajları, telefon şirketinden mesaj trafiğine erişimi olan herhangi biri ya da uygun donanımı olan diğer insanlar ele geçirebilir ve okuyabilir.

Borna: Aptalca. Peki ne yapmalıyım? Savaş zamanında olduğu gibi şifreli mesaj mı yazmalıyım?

Delir: Kimi durumlarda en eski ayakkabılar en rahat olanlardır.

Gönderilen SMS mesajlarına servis operatörleri ya da üçüncü kişiler, ucuz donanımlar aracılığıyla müdahale edebilir. Bu mesajlar, gönderenin ve alıcının telefon numaralarının yanı sıra mesajın içeriğini de taşır. Dahası SMS mesajları üçüncü kişiler tarafından kolayca değiştirilebilir ya da kopyalanabilir.

Siz ve alıcı arasında bir kodlama sistemi oluşturmayı düşünün. Kodlar haberleşmenizi daha güvenilir kılar ve haberleştiğiniz kişinin kimliğini doğrulamak için ek bir yol sağlar. Kodlama sistemi güvenli olmalıdır ve sık sık değiştirilmelidir.

SMS mesajları aktarıldıktan sonra bile erişilebilirdir:

- Birçok ülkede yasama (ya da diğer etkili kurumlar) ağ sağlayıcılarının, müşterileri tarafından gönderilen tüm yazılı mesajlarının uzun süreli kayıtlarını saklamalarını zorunlu kılar. Birçok durumda SMS mesajları sağlayıcılar tarafından iş, hesap tutmak ya da tartışmalı durumlarda kullanılmak amacıyla saklanır.
- Telefonunuzda kaydedilen mesajlar, telefonunuzu ele geçiren herhangi biri tarafından kolayca erişilebilirdir. Alınan ve gönderilen tüm mesajları doğrudan silmeyi düşünün.
- Bazı telefonların, arama ve yazılı mesaj geçmişinin kaydedilmesini devre dışı bırakma işlevi vardır. Bu özellikle hassas işler yapan kişiler için önemlidir. Telefonunuzun tüm işlevlerini bildiğinizden emin olun. Telefonunuzun kullanım kılavuzunu okuyun!

Sesli iletişim ve mesajlaşmanın ötesindeki işlevler

Cep telefonları, kendi işletim sistemleri ve kullanıcılara çeşitli hizmetler sunan indirilebilir uygulamalarıyla eksiksiz bir taşınabilir bilgisayara dönüşmektedir.

11. Bölüm: Akıllı telefonlar nasıl olabildiğince güvenli kullanılır ^[113], bu tür taşınabilir cihazlarla ilgili sorunları ele alır. İnternete bağlı olmak bazı imkanların yanı sıra önceki bölümlerde ele alınan riskleri de beraberinde getirmektedir.

Bazı eski cep telefonu modellerinin internet işlevi olmasa da veya çok az olsa da, aşağıda sunulan önlemleri incelemek yine de önemlidir. Uygun önlemleri aldığınızdan emin olmak için telefonunuzun kapasitesini tam olarak öğrenmelisiniz:

- Cep telefonunuza gizli dosyalarınızı ya da fotoğraflarınızı kaydetmeyin. **Bilgisayarınızdaki hassas dosyaları nasıl korursunuz** ^[41] başlıklı **4. Bölüm** ^[41]'de ele alındığı gibi, mümkün olduğunca kısa sürede onları güvenli bir konuma taşıyın.
- Telefonunuzun arama geçmişini, kayıtlı mesajları, adres defteri girdilerini, fotoğrafları vb. düzenli aralıklarla silin.
- Telefonunuzu internette gezinmek için kullanıyorsanız, bilgisayarınızda kullandığınıza benzer güvenlik uygulamalarını izleyin (örneğin, daima **HTTPS** ^[103] gibi şifrelenmiş bağlantılar üzerinden bilgi gönderin).
- Telefonunuzu bir bilgisayara kötü amaçlı yazılımlardan temizlenmiş olduğundan eminseniz bağlayın. **Bilgisayarınızı kötü amaçlı yazılımlara ve hacker'lara karşı nasıl korursunuz** ^[56] başlıklı **1. Bölüm** ^[56]'e bakınız.
- Cep telefonu zil sesleri, duvar kâğıtları, **java uygulamaları** ^[176] gibi istenmeyen ve beklenmedik bir kaynaktan size ulaşan, bilinmeyen ve doğrulanmamış programları kabul etmeyin ve telefonunuza kurmayın. Bunlar virüs, kötü amaçlı yazılım ya da casusluk programı içerebilir.
- Telefonunuzun davranışlarını ve işlevlerini gözlemleyin. Bilinmeyen programlara ve çalışan işlemlere, yabancı mesajlara ve istikrarsız işlemlere bakın. Telefonunuzdaki özelliklerin ve uygulamaların bazılarını bilmiyorsanız ya da kullanmıyorsanız devre dışı bırakın ya da yapabiliyorsanız kaldırın.
- Tıpkı bilgisayarınızı kullanırken olduğu gibi, şifre istemeyen WiFi erişim noktalarına cep telefonunuzla bağlanırken dikkatli olun. Cep telefonları temelde bilgisayarlar gibidir ve bu nedenle bilgisayar ve internetin zayıflıkları ve güvenlik açıkları cep telefonları için de geçerlidir.
- Infrared (IrDA)** ^[177], **Bluetooth** ^[178] ve kablosuz Internet (WiFi) gibi iletişim kanallarının, bunları kullanmadığınız zamanlarda, kapalı ver devre dışı olduğundan emin olunuz. Sadece gerekli olduklarında açınız. Sadece güvenli durumlarda ve konumlarda kullanınız. İzlenmesi görece daha kolay bir iletişim biçimi olduğundan Bluetooth kullanmamayı düşünün. Bunun yerine, telefonda kulaklıklara ya da bir bilgisayara veri aktarırken bir kablo kullanın.

Okuma önerileri

- The Mobile Advocacy Toolkit** ^[179], The Tactical Technology Collective tarafından yayınlandı. Bu yazı, farklı konuların yanı sıra, **cep telefonlarının güvenliği** ^[180] üzerine eksiksiz açıklamalar ve rehberler içerir. Ayrıca çok sayıda araç ve bu araçların kullanımı üzerine örnekler içermektedir.
- Security for Activists - A Practical Security Handbook for Activists and Campaigns** ^[181].
- A Guide to Mobile Phones – A short guide, for activists, to using mobile phones safely and securely** ^[182].
- MobileActive.org tarafından yayınlanan **A Guide to Mobile Security for Citizen Journalists** ^[183]
- A Brief Introduction to Secure SMS Messaging in MIDP - Nokia developer guide** ^[184]
- Phones used as spying devices** ^[185]

11. Akıllı telefonlar nasıl olabildiğince güvenli kullanılır

Cep telefonları nasıl olabildiğince güvenli kullanılır ^[186] başlıklı **10. Bölüm** ^[186]'de eski nesil cep telefonlarının, sesli haberleşme ve yazılı mesajlaşma (SMS/MMS) hizmetlerinin sorunları da dahil olmak üzere, güvenlik sorunlarını ele aldık. Bu telefonlar öncelikle (tamamen değilse de) arama ve veri aktarmak için taşınabilir ağırları kullanmaktadır.

Günümüzde teknolojik ilerlemeler, cep telefonlarının masaüstü ya da dizüstü bilgisayarlarinkine benzer hizmetleri ve özellikleri sağlayabileceği anlamına gelmektedir. Bu akıllı telefonlar, iletişim kurmak ve medya yakalayıp iletmek için birçok yeni yol sunmaktadır. Akıllı telefonlar, bu işlevleri yerine getirmek için sadece taşınabilir ağırları kullanmakla kalmaz ayrıca (internet kafedeki bir dizüstü bilgisayarın yaptığına benzer bir biçimde) bir WiFi bağlantısı aracılığıyla ya da taşınabilir ağ operatörü kullanarak veri bağlantısı aracılığıyla internete de bağlanabilir.

Akıllı telefonları küçük bilgisayar araçları olarak görmek daha uygundur. Dolayısıyla, bu araç kutusundaki diğer malzemeler, bilgisayarınız için olduğu kadar akıllı telefonunuz için de geçerlidir.

Akıllı telefonlar genellikle geniş bir işlevler dizisini destekler: web taraması, e-posta, internet üzerinden sesli ve anlık mesajlaşma; ses, görüntü ve fotoğraf yakalama, depolama ve aktarma; sosyal ağlar, çok kullanıcıli oyunlar, bankacılık ve diğer birçok etkinliği olanaklı kılar. Bununla beraber bu araçların ve özelliklerin birçoğu yeni güvenlik sorunlarına yol açar ya da var olan riskleri artırır.

Örneğin bazı akıllı telefonlar yerleşik küresel konumlama (**GPS** ^[187]) işlevine sahiptir ki bu; etkinliği kaldırılmadığı sürece işlevin, taşınabilir ağ operatörünüze ve telefonunuzda kullandığınız birçok uygulamaya (sosyal ağlar, haritalandırma,

tarama ve diğer uygulamalara) kesin konumunuzu sağlayabileceği anlamına gelir. Daha önce belirtildiği gibi cep telefonları, konum bilgilerinizi taşınabilir ağ operatörünüze (telefonun normal işlevinin bir parçası olarak) zaten aktarıyordu. Bununla beraber ek GPS işlevi konum bilgilerinizin kesinliğini artırmakla kalmaz, bu bilgilerin aktarılacağı yerlerin sayısını da artırır.

Cep telefonları nasıl olabildiğince güvenli kullanılır ^[186] başlıklı **10. Bölüm** ^[186]'de tartışılan cep telefonlarına eşlik eden tüm riskleri gözden geçirmek, bunların akıllı telefonların kullanımıyla da ilgili olması nedeniyle, yararlı olacaktır. **10. Bölüm** ^[186]; telefon görüşmelerinizin dinlenmesi, SMS ve diğer aramaların ele geçirilmesi ve SIM kartlarla ilgili sorunların yanı sıra pratik edebileceğiniz en iyi uygulamaları kapsamaktadır.

Bu bölümde akıllı telefonların ortaya koyduğu ek güvenlik sorunlarına göz atacağız.

Çantalar, Cüzdanlar, Akıllı Telefonlar

Çantamızı ya da cüzdanımızı korumamızın önemi konusunda içgüdüsel bir anlayışımız vardır çünkü onların içine çok hassas bilgiler depolanmıştır ve onları kaybetmek mahremiyetimizden ve güvenliğimizden ödün vermek olacaktır. İnsanlar akıllı telefonlarında taşıdıkları kişisel bilgilerin miktarı konusunda daha az farkındalığa sahiptir. Bir telefonu kaybetmenin bir riskten çok bir ayrıntı olduğu düşünülür. Akıllı telefonunun daima bir ağa bağlı bir bilgisayar aracı olduğunu ve daima sizinle birlikte oraya buraya taşındığını düşünürseniz; izole edilmiş, pasif bilgilerin taşıyıcısı olan bir cüzdan ile akıllı telefon gibi aktif ve interaktif bir araç arasındaki farkın önemini anlayabilirsiniz.

Basit bir uygulama bunu sergilemeye yardım edebilir:

Çantanızın ya da cüzdanınızın içindekileri boşaltın ve hassas şeyleri göz önünde bulundurun. Genellikle şunları bulabilirsiniz: - Sevdiklerinizin resimleri (~5 resim) - Kimlik kartları (ehliyet, üyelik kartları, sosyal güvenlik kartı) - Sigorta ve sağlık bilgileri (~2 kart) - Para (~5 banknot) - Kredi kartları, bankamatik kartları (~3 kart)

Şimdi akıllı telefonunuzun içeriğini inceleyin. Tipik bir akıllı telefon kullanıcısı yukarıdakilerden bazılarını daha yüksek miktarlarda ve bazı durumlarda da çok daha değerli şeyleri bulabilir:

- Sevdiklerinizin resimleri (~100 resim)
- E-posta uygulamaları ve bunların şifreleri
- E-postalar (~500 e-posta)
- Videolar (~50 video)
- Sosyal ağ uygulamaları ve bunların şifreleri
- Bankacılık uygulamaları (banka hesaplarına erişimle birlikte)
- Hassas belgeler
- Hassas iletişim kayıtları
- Hassas bilgilerinize canlı bir bağlantı

Akıllı telefonları kullandıkça onlara eşlik eden riskler hakkında daha fazla bilgi sahibi olmanız ve uygun önlemleri almanız gerekir. Akıllı telefonlar, kişisel verilerinizi dışarıya ileten güçlü hoparlörler ve dağıtıcılardır. Akıllı telefonlar, standart olarak, olabildiğince çok bağlantı ve sosyal ağ hizmetlerine bağlantı sağlamak için tasarlanmışlardır. Bunun nedeni kişisel bilgilerinizin derlenebilir, taranabilir ve satılabilir değerli bilgiler olmasındandır.

Veri kayıpları nasıl kurtarılır ^[43] başlıklı **5. Bölüm** ^[43]'de verileri yedeklemenin önemini ele aldık. Bu, özellikle akıllı telefonlar için geçerlidir. En önemli verilerinizi (kişiler listesi gibi) güvenli bir yere yedeklemeden telefonunuzu kaybederseniz bu bir felaket olabilir. Verilerinizi yedeklemenin yanı sıra verilerinizi nasıl kurtaracağınızı biliyor olduğunuzdan da emin olun. Atmak zorunda olduğunuz adımların basılı bir kopyasını saklayın, böylece acil bir durumda bu adımları hızla uygulayabilin.

Bu bölüme akıllı telefonların bazı temel özelliklerini tanıtarak başlayacağız: temel bazı platformların betimlemesi, bilgilerinizi ve iletişiminizi güvence altına almak için bazı temel kurma prosedürleri. Bu bölümün geriye kalan kısımları akıllı telefonların yaygın kullanımıyla ilgili belirli önlemleri ele alacaktır. Ardından gelen kısımlar aşağıda verilenin güvenlik boyutunu ele alacaktır:

Platformlar, Kurma ve Yükleme

Platformlar ve İşletim Sistemleri

Bu kitabın yazımı sırasında kullandığımız en yaygın akıllı telefonlar Apple'ın iPhone'u, Google'ın Android'i ve onları Blackberry ve Windows Phone izliyor. Android ve diğer işletim sistemleri arasındaki en önemli farklılık Android'in, çoğu zaman, Açık Kaynak Kodlu (**FOSS** ^[188]) bir sistem, yani kullanıcının bilgilerini ve iletişimini düzgün bir biçimde koruyup korumadığını doğrulamak için bağımsız olarak denetlemeye izin veren bir işletim sistemi olmasıdır. Bu işletim sistemi ayrıca bu platform için güvenlik uygulamalarının geliştirilmesini de kolaylaştırır. Güvenlik farkındalığına sahip birçok programcı, kullanıcı güvenliğini göz önünde bulundurarak Android uygulamaları geliştirir. Bölümün ilerleyen kısımlarında bunlardan bazılarının üzerinde durulacaktır.

Kullandığınız akıllı telefonun türü ne olursa olsun, internete bağlanan ve **GPS** ^[170] ya da kablosuz internet kapasitesi gibi özellikleri beraberinde taşıyan bir telefonu kullanırken farkında olmanız gereken sorunlar vardır. Bu bölümde Android platformlu araçlar üzerine odaklanacağız, çünkü yukarıda da belirttiğimiz gibi, Android platformlu araçlarda veri ve iletişimi korumak daha kolaydır. Bununla birlikte, bu bölümde temel kurma rehberleri ve Android telefonlarından farklı araçların bazı

uygulamaları da verilecektir.

Blackberry telefonları 'güvenli' mesajlaşma ve e-posta araçları olarak sunulmuştu. Bunun nedeni mesajların ve e-postaların, potansiyel kulak misafirlerinin erişimine engel olacak şekilde, Blackberry sunucuları aracılığıyla güvenli bir biçimde aktarılmasıydı. Ne yazık ki, hükümetler, potansiyel terörizme ve örgütlü suça karşı güvenlik gereksinimine vurgu yaparak, gittikçe daha çok bu iletişim bilgilerine erişim talep etmektedir. Hindistan, Birleşik Arap Emirliği, Sudi Arabistan ve Lübnan, Blackberry araçlarının kullanımını inceleyen ve ülkelerindeki kullanıcıların bilgilerini talep eden hükümetlerden birkaçıdır.

Eski Nesil Cep Telefonları

Cep telefonlarının bir başka kategorisi sık sık 'Eski Nesil Cep Telefonları' olarak adlandırılır (örneğin, Nokia 7705 Twist ya da Samsung Rogue). Kısa bir süre önce eski nesil cep telefonları bazı akıllı telefonlarınkileri de içerecek şekilde işlevlerini arttırdı. Ancak genel olarak bu telefonların işletim sistemleri daha az erişilebilirdir ve bu nedenle de güvenlik uygulamaları ve geliştirme için var olan olanaklar sınırlıdır. Her ne kadar burada ele aldığımız önlemler bu tür telefonlar için de anlamlı olsa da, eski nesil cep telefonlarına özel olarak atıfta bulunmayacağız.

Operatör markalı ve kilitlenmiş akıllı telefonlar

Akıllı telefonlar genellikle operatör markalı ya da kilitlenmiş olarak satılır. Akıllı telefonları kilitlemek şu anlama gelir: cihaz tek bir taşıyıcıyla işletilebilir ve bu taşıyıcı, cihazı aldığınızda beraberinde gelen SIM karttır. Taşınabilir ağ operatörleri kendi donanım yazılımını ya da yazılımını yükleyerek bir telefonu üretir ve markalaştırır. Ayrıca bazı işlevleri çalıştıramaz kılabilir ya da başkalarını ekleyebilirler. Markalaştırma, şirketlerin akıllı telefon kullanımını yönlendirerek, çoğu zaman da telefonunuzu nasıl kullandığınız hakkında veri toplayarak ya da akıllı telefonunuza uzaktan erişimi mümkün kılarak gelir arttırmak için kullanılan bir araçtır.

Bu nedenlerden dolayı, mümkünse operatör markasız akıllı telefon almanızı tavsiye ediyoruz. Kilitlenmiş bir telefon, tüm verilerinizi, veri akışlarınızı merkezileştiren tek bir taşıyıcıya yönlendirildiğinden ve verileri farklı taşıyıcılar üzerinden dağıtmak için SIM kartlarını değiştirmeyi olanaksız kıldığından daha yüksek bir risk kaynağıdır. Telefonunuz kilitlenmiş ise güvendiğiniz birinden onun kilidini açmasını isteyin.

Genel Kurulum

Akıllı telefonların aracın güvenliğini kontrol eden birçok ayarı vardır. Akıllı telefonunuzun nasıl kurulduğuna dikkat etmeniz önemlidir. Aşağıdaki Uygulama Rehberleri'nde sizi bazı akıllı telefon güvenlik ayarları konusunda uyaracağız. Öyle ki bazı akıllı telefonların güvenlik ayarları bulunsa da bunlar öntanımlı olarak aktif değildir. Yahut bazı akıllı telefonlarda bu güvenlik ayarları öntanımlı olarak aktif ve telefonunuzu korumasız hale getirir.

Uygulama: [Android için Temel Kurulum Rehberi](#) ^[189] ile uygulamaya başlayın

Uygulamaları kurmak ve güncellemek

Akıllı telefonunuza yeni yazılım yüklemenin alışlagelmiş yolu, iPhone Appstore'a ya da Google Play store'a kullanıcı kimlik bilgileriyle giriş yapmak ve istediğiniz uygulamayı indirerek kurmaktır. Giriş yaparak, kullanıcı hesabınızı çevrimiçi dükkânı kullanmanızla ilişkilendirmiş olursunuz. Uygulama dükkânının sahipleri, kullanıcının tarama geçmişinin ve uygulama tercihlerinin kayıtlarını tutar.

Resmî çevrimiçi dükkânlarda sunulan uygulamalar, varsayımsal olarak, dükkân sahiplerince (Google ya da Apple) onaylanmışlardır ama gerçekte bu onaylama, uygulamanın telefonunuza kurulduktan sonra neler yapacağına karşı çok zayıf bir güvence sağlar. Örneğin bazı uygulamalar telefonunuza kurulduktan sonra adres defterinizi kopyalar ve dışarıya gönderir. Android telefonlar, her uygulama kurulumu aşamasında, bu uygulamalar kullanılırken nelere izin verildiğini size onaylatmak zorundadır. Hangi izinlerin istendiğine ve bu izinlerin kurmakta olduğunuz uygulamanın işleviyle anlamlı bir uyum içerisinde olup olmadığına çok dikkat etmelisiniz. Örneğin bir "haber okuma" uygulaması kurmayı düşünüyorsanız ve bu uygulamanın kişiler listenizi, taşınabilir veri bağlantısı üzerinden üçüncü kişilere gönderme hakkını talep ettiğini fark ederseniz, uygun erişim ve haklara sahip başka bir uygulama aramalısınız.

Android uygulamaları resmî Google kanalları dışındaki kaynaklarda da sunulmaktadır. Bu indirme sitelerini kullanmak için tek yapmanız gereken *Güvenlik ayarları*'nızdaki *Bilinmeyen Kaynaklar* kutusunu işaretlemenizdir. Bazı kullanıcılar Google'la çevrimiçi teması asgariye indirmek için bu alternatif siteleri gözden geçirmek isteyebilir. Alternatif dükkânlardan bir tanesi, sadece [FOSS](#) ^[7] uygulamaları sunan **F-Droid** ^[190] dir ('Free Droid'). Ayrıca bir siteden herhangi bir uygulama indirmeden önce ona güveniyor olmanız gerektiğini lütfen hatırlayın. Deneyimsiz kullanıcılar için Google Play dükkânını kullanmalarını tavsiye ederiz.

Uygulamalara erişmek için çevrimiçi olmak istemiyorsanız, uygulamaları başkalarının telefonundan Bluetooth aracılığıyla [.apk](#) ^[191] ('android uygulama paketi'nin kısaltılmış hali) dosyalarını göndererek aktarabilirsiniz. Alternatif olarak .apk dosyalarını aracınızın Micro SD kartına indirebilir ya da bir usb kablo ile bir PC'den karta aktarabilirsiniz. Dosyaları aldıktan sonra dosya adına uzun süre tıkladığınızda uygulamayı kurmak için uyarılacaksınız. (**Not:** özellikle bluetooth kullanırken dikkatli olun - [10. Bölüm](#) ^[186]'deki [Sesli iletişim ve mesajlaşmanın ötesindeki işlevler](#) ^[192] kısmını okuyun).

Akıllı Telefonlar Aracılığıyla İletişim (Sesli İletişim ve

Mesajlar)

Güvenle Konuşmak

Temel Telefon işlevi

Cep telefonları nasıl olabildiğince güvenli kullanılır ^[186] başlıklı **10. Bölüm** ^[186]'ün **Temel işlevler, takip edilebilirlik ve anonimlik** ^[193] kısmında sesli iletişim için cep telefonu operatör ağını kullanırken dinlenmeniz riskini en aza indirmek için düşünceleriniz gereken farklı önlemleri tartışmıştık.

Akıllı telefonunuz aracılığıyla, taşınabilir veri bağlantıları ya da WiFi üzerinden interneti kullanmak, iletişim için daha güvenli yollar sağlayabilir; örneğin VoIP kullanmak ve bu iletişim kanalını güvenli hale getirmek için gerekli araçlara başvurmak gibi... Bazı akıllı telefon araçları bu güvenliği **VoIP** ^[194]'in bile ötesine, cep telefonu görüşmelerine de taşıyabilir (bakınız aşağıda **Redphone**).

Burada birkaç aracı ve onların olumlu ve olumsuz yanlarını listeliyoruz:

Skype

En popüler ticari VoIP uygulaması olan **Skype** ^[195], tüm akıllı telefon platformları için kullanılabilir ve kablosuz bağlantınız güvenilirse iyi de işlemektedir. Taşınabilir veri bağlantılarında Skype daha az güvenilirdir.

İnternet iletişiminizin gizliliği nasıl korunur ^[196] başlıklı **7. Bölüm** ^[196]'ün **Diğer internet iletişim araçlarını güvenli kılmak** ^[197] kısmında Skype kullanmanın risklerini ve mümkünse neden kullanmaktan kaçınmak gerektiğini ele almıştık. Özet olarak Skype Açık Kaynak Kodlu bir yazılım değildir ve bu, Skype'ın güvenlik düzeyini bağımsız olarak sınamayı güçleştirir. Dahası Skype, onu ne zaman ve nereden kullandığınızı bilmekte ticarî çıkarları olan Microsoft'a aittir. Skype yasa uygulayıcı makamların tüm iletişim geçmişinize geriye dönük olarak erişimine izin de verebilir.

Diğer VoIP

VoIP'i kullanmak genel olarak ücretsizdir (ya da cep telefonlarıyla arama yapmaktan çok daha ucuzdur) ve çok az veri izi bırakır. Gerçekten de güvenli kılınmış bir VoIP konuşması en güvenli iletişim yolu olabilir.

Farklı VoIP hizmetleri için basit kurma sihirbazlarıyla birlikte sunulan, **CSipSimple** ^[198], Android telefonlar için iyi ve güçlü bir VoIP programıdır.

Open Secure Telephony Network (OSTN) ^[199] ve Guardian projesi tarafından sağlanan bir sunucu olan **ostel.me** ^[200], günümüzde sesli olarak iletişimin en güvenli araçlarından birini sunmaktadır. VoIP iletişimlerinizi için sunucu işleten kuruluşu bilmek ve güvenmek ciddi bir değerlendirmeyi gerektirir.

CSipSimple kullanırken hiçbir zaman doğrudan iletişim partnerinizle iletişim kurmazsınız, bunun yerine tüm verileriniz Ostel sunucusu aracılığıyla yönlendirilir. Bu, verilerinizin izini sürmeyi ve kimle konuştuğunuzu bulmayı güçleştirir. Dahası Ostel, giriş yapmanız için gerekli olan hesap bilgileriniz dışında hiçbir veriyi elinde tutmaz. Tüm konuşmanız güvenli bir biçimde şifrelenir ve hatta gizlemesi oldukça zor olan meta verileriniz bile, trafik ostel.me sunucusu aracılığıyla iletildiğinden, okunması güç hale gelir. CSipSimple'ı ostel.me sitesinden indirirseniz, programınız ostel.me'yle kullanılmak üzere önceden düzenlenmiş olarak gelecektir; bu da uygulamanın kurulumunu ve kullanımını oldukça kolaylaştırmaktadır.

RedPhone ^[201], bu uygulamayı işleten iki araç arasında gönderilen sesli iletişim verilerini şifreleyen, ücretsiz ve Açık Kaynak Kodlu bir yazılımdır. Program kendisini normal arama ve kişiler şemanızla bütünleştirdiğinden kurulumu ve kullanımı oldukça kolaydır. Ama konuşmak istediğiniz kişilerin de RedPhone'u kurmuş ve kullanıyor olması gerekir. Kullanım kolaylığı için RedPhone, tanımlayıcınız olarak (diğer VoIP servislerinde kullanıcı adı gibi) sizin cep numaranızı kullanır. Ancak bu nedenle Redphone'un ürettiği trafiği çözümlemek ve cep numaranız aracılığıyla size kadar izini sürmek çok daha kolay hale gelir. RedPhone merkezî bir sunucu kullanmaktadır, ki bu bir merkezileşme sorunudur ve böylece RedPhone'u güçlü bir konuma (bu verilerin üzerinde denetim sahibi olma konumuna) getirir.

CSipSimple, Ostel.me ve Redphone için Uygulama Rehberleri hazırlanmaktadır. Daha fazla bilgiye yukarıdaki bağlantıları takip ederek ulaşabilirsiniz.

Güvenli Mesaj Gönderme

Akıllı telefonunuzla SMS gönderirken, anlık mesajlaşma ya da sohbet programları kullanırken bazı önlemler almalısınız.

SMS

10. Bölüm ^[186]'de (**Yazılı iletişim** ^[202] kısmında) betimlendiği gibi, SMS iletişimi standart olarak güvenli değildir. Taşınabilir telekomünikasyon ağına erişimi olan herkes bu mesajları kolayca ele geçirebilir ve bu, birçok durumda her gün meydana gelen bir şeydir. Kritik durumlarda güvenli olmayan SMS mesajı göndermeye güvenmeyin. SMS mesajlarının sahipliğini kanıtlamanın hiçbir yolu yoktur bu nedenle SMS'in gönderimi aşamasında mesajın içeriğinin değiştirilip değiştirilmediğini ya da mesajı gönderen kişinin olduğunu iddia ettiği kişi olup olmadığını bilmek mümkün değildir.

SMS'leri Güvenli Kılmak

TextSecure ^[203] Android telefonlar için güvenli SMS gönderimi ve alımı için tasarlanmış bir **FOSS** ^[7] aracıdır. Hem şifrelenmiş hem de şifrelenmemiş mesajlarla çalıştığından bu uygulamayı standart SMS uygulamanız olarak kullanabilirsiniz. Şifrelenmiş mesajları alıp vermek için, bu araç hem göndericide hem de mesajın alıcısında kurulu olmalıdır. Bu nedenle düzenli olarak iletişim içinde olduğunuz kişilerin de bu uygulamayı edinmesini sağlamanız gerekir. TextSecure bir başka TextSecure kullanıcısından şifreli bir mesaj aldığını otomatik anlar. Ayrıca birden fazla kişiye şifreli mesaj göndermenize izin verir. Mesajlar, mesajın içeriğine zarar verilmesini neredeyse olanaksız kılarak, otomatik olarak imzalanır. TextSecure Uygulama Rehberi'nde bu aracın özellikleri ve nasıl kullanılacağı detaylı bir şekilde açıklanmıştır.

Uygulama: [TextSecure Rehberi](#) ^[204] ile uygulamaya başlayın

Güvenli Çevrimiçi Sohbet

Telefonunuzla anlık mesajlaşma ve çevrimiçi sohbet, dinlenme riski taşıyan birçok bilgi üretebilir. Bu haberleşmeler düşmanlarınız tarafından ileriki bir tarihte size karşı kullanılabilir. Bu nedenle anlık mesajlaşma ve çevrimiçi sohbet sırasında telefonunuza yazarken neleri ifşa ettiğiniz konusunda son derece şüpheci olmalısınız.

Güvenli çevrimiçi sohbet ve anlık mesajlaşma yolları vardır. Bunun en iyi yolu diğer uçtaki kişinin mesajlaşmak istediğiniz kişi olduğundan emin olmanızı sağlayan uçtan uca şifrelemedir.

Biz Android telefonlar için güvenli bir yazılı sohbet uygulaması olan **Gibberbot** ^[205]'u tavsiye ediyoruz. Gibberbot *Off-the-Record* ^[94] Mesajlaşma protokolüyle birlikte sohbetini için basit ve güçlü bir şifreleme sunar. Bu şifreleme, hem kimlik doğrulama özelliği (doğru kişiyle sohbet ettiğinizi doğrulayabilirsiniz) hem de her seans için bağımsız güvenlik sunar, öyle ki bir sohbet seansının şifrelemesinin gizliği ihlal edilse bile geçmiş ve gelecek seanslar güvenli olarak kalacaktır.

Gibberbot, Orbot'la birlikte çalışacak şekilde tasarlanmıştır. Böylece çevrimiçi sohbet mesajlarınız **Tor** ^[111] anonimleştirici ağından yönlendirilebilir. Bu, mesajlarınızın izini sürmeyi ya da çevrimiçi sohbetin gerçekleştiğini bile anlamayı oldukça güçleştirir.

Uygulama: [Gibberbot Rehberi](#) ^[206] ile uygulamaya başlayın

ChatSecure ^[207] uygulaması, iPhone'lar için de aynı özellikleri sunar ancak onu **Tor** ^[111] ağıyla birlikte kullanmak kolay değildir.

ChatSecure için bir Uygulama Rehberi hazırlanmaktadır. Bu arada ChatSecure'ün [anasayfasında](#) ^[207] daha fazla bilgi bulunabilir.

Hangi uygulamayı kullanırsanız kullanın çevrimiçi sohbet için hangi hesabı kullanacağınızı daima göz önünde bulundurun. Örneğin Google Talk kullandığınızda, kimliğiniz ve sohbet seansının zamanı Google için bilinir hale gelir. Ayrıca görüştüğünüz kişilerle, sohbet geçmişini, özellikle şifrelenmemişse, kaydetmemek üzere anlaşın.

Akıllı Telefonunuzda Bilgi Depolamak

Akıllı telefonların geniş veri depolama kapasiteleri vardır. Ne yazık ki, araçlarınızda depolanan bilgilere üçüncü kişiler tarafından uzaktan ya da telefona fiziksel olarak ulaşarak kolayca erişilebilir. Bu bilgilere uygun olmayan erişimi azaltmak için bazı temel önlemler **Android için Temel Kurulum Rehberi** ^[189]'nde açıklanmıştır. Dahası belirli araçları kullanarak telefonunuzdaki herhangi bir hassas bilgiyi şifrelemek için adımlar atabilirsiniz.

Veri şifreleme araçları

Android Privacy Guard (APG) ^[208], dosyalar ve e-postalar için OpenPGP şifrelemesine izin verir. Bu, hem telefonunuzdaki hem de e-posta ile gönderdiğiniz dosyaları ve belgeleri güvenli olarak korumak için kullanılabilir.

Uygulama: [APG Rehberi](#) ^[208] ile uygulamaya başlayın

Cryptonite ^[209] bir başka **FOSS** ^[7] dosya şifreleme aracıdır. Cryptonite, kurulu donanım yazılımı ile gelen "root" edilmiş Android telefonlar için daha gelişmiş özelliklere sahiptir. Daha fazla bilgi için [İleri Düzey Akıllı Telefon Kullanımı](#) ^[210] kısmına bakınız.

Uygulama: [Cryptonite Rehberi](#) ^[211] ile uygulamaya başlayın

Şifreleri güvenli olarak saklama

Keepass kullanarak gereksinim duyduğunuz tüm şifreleri tek bir güvenli ve şifreli dosyada saklayabilirsiniz. Diğer bütün şifrelere erişmek için tek bir genel şifreyi hatırlamanız gerekecektir. Keepass'le sahip olduğunuz her bir hesap için, güçlü şifreler kullanabilirsiniz; Keepass sizin için bu şifreleri hatırlayacaktır. Ayrıca Keepass yeni şifreler yaratmak için kullanılan bir şifre üreticisiyle birlikte gelmektedir. Keepass şifre veri tabanınızı, telefonunuz ve bilgisayarınız arasında senkronize edebilirsiniz. Biz, sadece cep telefonunuzda kullandığınız şifreleri senkronize etmenizi tavsiye ediyoruz. Bilgisayarınızda daha küçük bir ayrı şifre veri tabanı yaratabilirsiniz ve akıllı telefonunuzda kullandığınız tüm şifreleri de içeren bütün bir veri tabanıyla uğraşmak yerine bu ayrı olanı senkronize edebilirsiniz. Ayrıca tüm şifreleriniz bir genel şifreyle korunuyor

olduğundan KeePass veri tabanınız için oldukça güçlü bir şifre kullanmanız çok önemlidir. Bakınız **Güvenli şifreler nasıl oluşturulur ve muhafaza edilir** ^[37] başlıklı **3. Bölüm** ^[37].

Uygulama: **KeePassDroid Rehberi** ^[212] ile uygulamaya başlayın

Akıllı Telefonlardan E-posta Göndermek

Bu kısımda akıllı telefonlarla e-posta kullanımını kısaca ele alacağız. Temel e-posta güvenliğini tartıştığımız **7. Bölüm: İnternet iletişiminin gizliliği nasıl korunur** ^[196]'daki , **E-postanızı güvenli kılmak** ^[213] ve **E-postaların izlendiğinden şüphelenildiğinde yapabilecekleriniz üzerine ipuçları** ^[101] başlıklı kısımlarına bakmanızı öneriyoruz.

İlk olarak e-postanıza erişmek için akıllı telefonunuzu kullanmanızın gerekli olup olmadığını düşünün. Bir bilgisayarı ve onun içeriğini güvenli kılmak, akıllı telefon gibi taşınabilir bir araca göre genellikle daha basittir. Bir akıllı telefon çalınmaya, izlenmeye ve saldırılara karşı daha açıktır.

E-postanıza erişmek için akıllı telefonunuzu kullanmanız mutlaka gerekliyse riski azaltmak için yapabileceğiniz bazı şeyler var.

- E-postanıza erişimin öncelikli aracı olarak akıllı telefona güvenmeyin. Bir e-posta sunucusundan e-posta indirmek (ve silmek) ve onları sadece akıllı telefonunuza depolamak tavsiye edilmez. E-posta uygulamanızı e-postaların sadece kopyalarını kullanacak şekilde kurabilirsiniz.
- Bazı kişilerle iletişiminizde e-posta şifrelemeyi kullanıyorsanız, bu uygulamayı akıllı telefonunuza da kurmayı değerlendirin. Bunun ek faydası, telefon yanlış ellere düşerse, şifrelenmiş e-postalar sır olarak kalacaktır.

Gizli şifreleme anahtarınızı taşınabilir aracınıza depolamak riskli görünebilir. Ancak taşınabilir aracınızdan güvenli olarak şifrelenmiş e-postaları gönderebilme ve depolamanın avantajı riskten daha ağır basabilir. Akıllı telefonunuzda kullanmak için sadece taşınabilir aracınız için (**APG** ^[208] kullanarak) bir şifre anahtarı oluşturmayı düşünün, böylece kişisel şifre anahtarınızı bilgisayarınızdan taşınabilir aracınıza kopyalayamazsınız. Unutmayın ki bu, iletişimde olduğunuz kişilerin de e-mailleri sadece taşınabilir aracınız için kullandığınız şifre anahtarını kullanarak şifrelemelerini gerektirmektedir.

Uygulama: **K9 ve APG Rehberi** ^[214] ile uygulamaya başlayın

Akıllı Telefonlarla Medya Yakalamak

Akıllı telefonunuzla fotoğraf, video ya da ses yakalamak önemli olayları belgelemenin ve paylaşmanın güçlü araçlarıdır. Bununla beraber fotoğraflananın, filme çekilenin ya da sesi kaydedilenin mahremiyetine ve güvenliğine saygı göstermek ve dikkat etmek de önemlidir. Örneğin önemli bir olayın fotoğraflarını çekiyorsanız ya da görüntüsünü ya da sesini kaydediyorsanız, telefonunuz yanlış ellere geçerse bu sizin için ya da kayıtlarda yer alan kişiler için tehlikeli olabilir. Bu durumda şu tavsiyeler yararlı olabilir:

- Kaydedilmiş medya dosyalarını korumalı çevrimiçi konuma güvenli olarak yüklemek için bir mekanizmaya sahip olun ve kaydettikten sonra telefonunuzdan bunları hemen (ya da mümkün olduğunca çabuk) silin.
- Fotoğraflarda ya da videolarda görünen kişilerin yüzlerini gizlemek için ya da sesli ya da görüntülü kayıtlardaki seslerini bozmak için araçlar kullanın ve medya dosyalarının sadece bu gizlenmiş ve bozulmuş kopyalarını taşınabilir cihazınızda depolayın.
- Medya dosyalarındaki zaman ve yerle ilgili meta bilgileri koruyun ya da silin.

Guardian Project ^[215], fotoğraflardaki yüzleri bulmak ve bulanıklaştırmak için **ObscuraCam** ^[216] adlı bir **FOSS** ^[7] uygulaması yarattı. Elbette bulanıklaştırma modunu ve neyi bulanıklaştıracağınızı seçebilirsiniz. ObscuraCam orjinal fotoğrafları da siler ve kaydettiğiniz medyayı yüklemek için bir sunucu belirlediyseniz, onları yüklemek için kolay bir işlem sunar.

Uygulama: **Obscuracam Rehberi** ^[217] ile uygulamaya başlayın

Bu metnin yazımı sırasında insan hakları örgütü **Witness** ^[218], Guardian Project'le birlikte yukarıda belirtilen üç sorun üzerine çalışmaktadır.

Akıllı Telefonlardan İnternete Güvenli Erişim

İnternet iletişiminizin gizliliği nasıl korunur ^[196] başlıklı **7. Bölüm** ^[196]'de ve **İnternette nasıl anonim kalınır ve internet sansürü nasıl asılır** ^[110] başlıklı **8. Bölüm** ^[110]'de ele aldığımız gibi, internetteki içeriğe erişim ya da fotoğraf veya video gibi malzemeleri çevrimiçi yayınlamak, kim olduğunuz ve nerede, ne yapıyor olduğunuz hakkında birçok iz bırakır. Bu sizi risk altına sokabilir. Akıllı telefonunuzu internet üzerinden iletişim için kullanmanız bu riski büyütür.

WiFi ya da Taşınabilir Veri Üzerinden Erişim

Akıllı telefonlar internete nasıl erişebileceğinizi denetim altında tutmanıza şu şekillerde izin verir: (bir internet kafede olduğu gibi) bir erişim noktası tarafından sağlanan kablosuz bağlantı aracılığıyla ya da GPRS, EDGE, ya da UMTS gibi taşınabilir ağ operatörlerinin sağladığı taşınabilir veri bağlantısı aracılığıyla.

Bir WiFi bağlantısı kullanmak, cep telefonu servis sağlayıcısıyla geride bırakıyor olabileceğiniz veri izlerini azaltmanızı sağlar (internet cep telefonu aboneliğinizle bağlanmadığınız durumlarda). Bununla beraber bazen bir taşınabilir ağ bağlantısı çevrim içi olmanın tek yoludur. Ne yazık ki taşınabilir ağ bağlantısı protokolleri (EDGE ya da UMTS gibi) açık standartlar değildir. Bağımsız geliştiriciler ya da güvenlik mühendisleri bu protokollerin taşınabilir ağ taşıyıcıları tarafından nasıl uygulandığını görmek için bunları inceleyemez.

Bazı ülkelerde taşınabilir erişim sağlayıcıları, internet servis sağlayıcılarından farklı yasalarla çalışır ki bu, devletlerin ve telefon şirketlerinin daha doğrudan gözetimiyle sonuçlanabilir.

Akıllı telefonlarla dijital iletişiminiz için hangi yolu seçtiğinizden bağımsız olarak, anonimleştirici araçları ve şifreleme araçlarını kullanarak verilerinizi ifşa etme riskini azaltabilirsiniz.

Anonimleştirme

Çevrimiçi içeriğe anonim olarak erişmek için Orbot adındaki Android uygulamayı kullanabilirsiniz. **Orbot** [219], Tor'un anonim ağı aracılığıyla internet iletişiminizi yönlendirir.

Uygulama: [Orbot Rehberi](#) [220] ile uygulamaya başlayın

Bir başka uygulama olan Orweb ise, proxy'ler kullanmak ve yerel tarama geçmişi tutmamak gibi gizliliği arttıran özellikleri olan bir internet tarayıcısıdır. Orbot ve Orweb birlikte internet filtrelerini ve güvenlik duvarlarını devre dışı bırakır ve anonim tarama hizmeti sunar.

Uygulama: [Orweb Rehberi](#) [221] ile uygulamaya başlayın

Proxyler

Firefox [13]'un taşınabilir sürümü **Firefox mobile** [222], trafiği proxy sunucularına yönlendiren proxy eklentileriyle donatılabilir. Trafiğiniz buradan istediğiniz siteye gider. Bu, sansür durumlarında yardımcı olabilir ama istemcinizle proxy'niz arasındaki bağlantının şifrelenmemiş olması durumunda siteye ulaşım isteğinizi ifşa edebilir. Firefox'la proxy kullanmayı kolaylaştıran **Guardian Project** [223] tarafından sunulan **Proxy Mobile** [224] eklentisini tavsiye ediyoruz. Bu, Firefox taşınabilir iletişimlerini Orbot'a yönlendirmenin ve **Tor** [111] ağını kullanmanın tek yoludur.

İleri Düzey Akıllı Telefon Güvenliği

Akıllı telefonunuza eksiksiz erişimi elde edin

Akıllı telefonların birçoğu, kurulu işletim sisteminin, üretici yazılımının ya da cep telefonu operatörlerinin programlarının izin verdiğinden daha fazlasına muktedirdir. Benzer bir biçimde akıllı telefonların bazı işlevleri, kullanıcıların bunları kontrol edememesi ya da değiştirememesi için "kilitlenmiş"tir, ve bunlar erişilemez olarak kalır. Birçok durumda bu işlevler akıllı telefon kullanıcıları için gereksizdir. Bununla beraber bir akıllı telefonun veri ve iletişim güvenliğini arttırabilecek bazı uygulamalar ve işlevler de vardır. Ayrıca güvenlik risklerinden kaçınmak için kaldırılacak bazı halihazırda var olan işlevler de mevcuttur.

Bu ve diğer nedenlerle bazı akıllı telefon kullanıcıları, zenginleştirilmiş işlevleri kurmalarına ya da uygun bulmadıkları diğer işlevleri kaldırmalarına ya da azaltmalarına izin verecek uygun ayrıcalıkları elde etmek için, akıllı telefonu çalıştıran çeşitli yazılımları ve programları değiştirmeyi tercih ederler.

Bir akıllı telefonda, hizmet sunucunuz ya da işletim sistemi üreticileri tarafından dayatılan sınırları aşma işlemi (Android araçlarda) 'rooting' ya da (iPhone ya da iPad gibi iOS araçlarda) 'jailbreaking' olarak adlandırılır. Genellikle başarılı bir rooting ya da jailbreaking, ek uygulamalar kurmak ve kullanmak, aksi halde kilitli olan düzenlemeler üzerinde değişiklikler yapmak ve akıllı telefonun veri depolaması ve hafızası üzerinde tam denetim için gereken tüm ayrıcalıklara sahip olmanız ile sonuçlanır.

UYARI: 'Rooting' ya da 'jailbreaking' geri döndürülemez işlemler olabilir ve yazılım yüklemesi ve yapılandırması konusunda deneyim gerektirir. Şunları göz önünde bulundurun:

- Akıllı telefonunuzu kalıcı olarak işlemez kılma riski vardır.
- Üretici ya da hizmet sunucunuzun garantisi geçersiz hale gelebilir.
- Bazı yerlerde bu işlem yasadışı olabilir.

Ama dikkatli olursanız 'root' edilmiş bir cihaz akıllı telefonunuzu daha güvenli kılmak için onun kontrolünü ele geçirmenin en doğrudan yoludur.

Alternatif Donanım Yazılımı

Donanım yazılımı belirli cihazlarla yakından ilişkili programlara işaret eder. Bunlar cihazın işletim sistemiyle iş birliği

içindedir ve akıllı telefonunuzun (hoparlör, mikrofon, kameralar, dokunmatik ekran, hafıza, anahtarlar, antenler, gibi) donanımının temel işlemlerinden sorumludur.

Android bir cihazınız varsa telefon üzerindeki denetiminizi daha da arttırmak için bir donanım yazılımı alternatifi kurmayı düşünebilirsiniz. Bir donanım yazılımı alternatifi kurmak için telefonunuzu “root” etmeniz gerektiğini aklınızda bulundurun.

Cyanogenmod ^[225], Android telefonlar için donanım yazılımı alternatifine örnektir; telefonunuzun sistem düzeyindeki (yani, telefon üreticisi ya da taşınabilir ağ operatörü tarafından kurulan) uygulamalarını kaldırmanıza izin verir. Bunu yaparak, cihazınızın izlenebileceği bir dizi yolu azaltabilirsiniz; örneğin bilginiz dışında servis sağlayıcınıza gönderilen veriler.

Dahası Cyanogenmod, bir OpenVPN uygulamasıyla birlikte gelmektedir, bu da sizi Open VPN’i manuel olarak kurmak zahmetinden kurtarır. VPN (Virtual Private Network/Sanal Özel Ağ) internet iletişiminizi güvenli “proxy” etmenin yollarından biridir (aşağıya bakınız).

Ayrıca Cyanogenmod, iletişim geçmişinizin akıllı telefonunuza kaydedilmediği anonimleştirilmiş bir tarama modu sunmaktadır.

Cyanogenmod birçok diğer özelliği beraberinde taşır. Ancak tüm Android cihazlar tarafından desteklenmemektedir. Daha fazla ilerlemeden [desteklenen cihazlar listesi](#) ^[226]’ne göz atın.

Bütün bölümlerin şifrlenmesi

Telefonunuz root edildiyse tüm veri depolamasını şifrelemeyi ya da bazı bilgilerinizi telefonunuzda korumak için akıllı telefonunuzda bir bölüm yaratmayı düşünebilirsiniz.

Luks Manager ^[227] kullanıcı dostu arayüzüyle bölümlerin kolay ve güçlü bir şekilde şifrlenmesine izin verir. Android cihazınıza önemli veriler depolamaya başlamadan önce bu aracı kurmanızı ve Luks Manager tarafından sağlanan Şifrelenmiş Bölümleri veri depolamak için kullanmanızı şiddetle tavsiye ediyoruz.

Whisper Systems projesi tüm Android cihazınızı şifrelemenize izin verecek **WhisperCore** ^[228] uygulamasını hazırlamaktadır.

Sanal Özel Ağ (VPN)

Bir VPN, cihazınız ve bir VPN sunucusu arasında internet aracılığıyla şifrelenmiş bir tünel sağlar. Bu bir tünel olarak adlandırılır çünkü https’ler gibi, diğer şifrelenmiş trafikten farklı olarak, tüm servisleri, protokolleri ve içeriği gizler. Bir VPN bağlantısı sadece bir kez kurulur ve sadece siz karar verdiğiniz zaman sona erer.

Tüm trafiğiniz proxy ya da VPN sunucusu üzerinden geçtiğinden bir aracının, etkinliklerinizi çözümlemek için sadece proxy’nize girmesi gerektiğini aklınızda bulundurun. Bu nedenle proxy ve VPN hizmeti sunan kurum ya da kişiler arasında dikkatlice seçim yapmak önemlidir. Veri akışınızı dağıtmanız, gizliliği ihlal edilmiş sistemlerin etkisini azaltacağından, farklı proxy’leri veya da VPN’leri kullanmanız ayrıca tavsiye edilebilir.

RiseUp VPN ^[229] sunucusunu kullanmanızı tavsiye ediyoruz. RiseUp VPN’i Cyanogenmod’u kurduktan sonra Android cihazlarda kullanabilirsiniz (bakınız yukarı). iPhone’larda da RiseUp VPN bağlantısını kurmak kolaydır – [buradan](#) ^[230] daha fazla bilgi edinebilirsiniz.

Terimler Sözlüğü

Bu bölümleri okurken karşılaşacağınız bazı teknik terimler aşağıda tanımlanmıştır:

- **Alan adı** - Bir web sitesi ya da internet servisi adresinin sözcük olarak adı; örneğin: securityinbox.org
- **Android**: Google tarafından akıllı telefonlar ve tabletler için geliştirilen GA Linux tabanlı, açık kaynak kodlu bir işletim sistemi.
- **APG**: Android Privacy Guard: OpenPGP şifrelemeye izin veren Android akıllı telefonlar için FOSS uygulaması. K9 Mail’e entegre edilebilir.
- **.apk dosyası**: Android uygulamaları için kullanılan dosya uzantısı.
- **App Store**: iPhone uygulamalarının bulunabileceği ve indirilebileceği verili depo.
- **Avast** - Ücretsiz bir anti-virüs aracı
- **Beyaz liste** - Diğer web siteleri otomatik olarak engellendiğinde bir tür erişime izin verilen sitelerin ya da internet servislerinin bir listesi
- **BlackBerry**: Research In Motion (RIM) tarafından geliştirilmiş BlackBerry işletim sistemini kullanan bir akıllı telefon markası.
- **Bluetooth** - Sabit ve taşınabilir cihazlardan kısa mesafeden veri alışverişi sağlayan fiziksel kablosuz iletişim

standartı. Bluetooth kısa dalga radyo aktarımını kullanır.

- **Booting** - Bir bilgisayar başlatma işlemi
- **CCleaner** - Windows işletim sistemi ve sizin tarafınızdan yakın bir geçmişte kullanılan programların sabit diskte bıraktığı potansiyel olarak hassas izleri ve geçici dosyaları ortadan kaldıran ücretsiz bir araç
- **CD Yazıcı** - Boş CD'lere yazabilen bir bilgisayar CD-ROM sürücüsüdür. *DVD yazıcıları* da aynı işi boş DVD'ler için yapabilir. *CD-RW* ve *DVD-RW sürücüler*i aynı CD-RW ya da DVD-RW disketlere birden fazla kez bilgi kaydedebilir ve silebilir.
- **Clam Win** - Windows için bir FOSS Anti-virus programı
- **Cobian Backup** - Yedekleme için bir FOSS aracı. Cobian'ın en son sürümleri kapalı kaynaklı ve ücretsizdir, ama önceki sürümleri FOSS'tur.
- **Comodo Firewall** - Ücretsiz bir güvenlik duvarı aracı
- **Cryptonite**: Android akıllı telefonlarda dosya şifrelemek için kullanılan bir FOSS uygulaması.
- **Çerez (Cookie)** - Tarayıcınız tarafından bilgisayarınıza kaydedilen ve belirli bir web sitesine bilgi depolamak ve sizi tanımlamak amacıyla kullanılabilen küçük bir dosya
- **Dijital imza** - Belirli bir dosyayı ya da mesajı gönderdiğini iddia eden kişinin gerçekten de o kişi olduğunu kanıtlamak için kullanılan şifreleme yöntemi
- **EDGE, GPRS, UMTS**: Açılımları 'Enhanced Data Rates for GSM Evolution', 'General Packet Radio Service', 'Universal Mobile Telecommunications System' olan; taşınabilir cihazların internete bağlanmasını sağlayan teknolojiler.
- **Enigmail** - Thunderbird e-posta programının şifrelenmiş ve dijital imzalı e-postalar gönderip almasını sağlayan bir eklentisi
- **Eraser** - Bilgisayarınızdan ya da çıkarılabilir depolama aygıtınızdan güvenli bir biçimde ve kalıcı olarak bilgi silen bir araç.
- **F-Droid**: Birçok FOSS Android uygulamasının bulunabileceği ve indirilebileceği alternatif bir depo
- **Firefox** - Microsoft Internet Explorer'a bir alternatif oluşturan popüler FOSS web tarayıcısı
- **Fiziksel tehdit** - Bu kitapta sözü edilen bağlamda, bilgisayarınızın donanımına doğrudan erişimi olan diğer insanlardan ya da kazalar veya doğal felaketler gibi diğer fiziksel risklerden kaynaklanan hassas bilgilerinize yönelik herhangi bir tehdit.
- **Gibberbot**: (Google Talk'un da kullandığı) XMPP protokolü üzerinden güvenli sohbeti sağlayan Android için bir FOSS uygulaması. Off-the-Record eklentisi ile uyumludur ve Orbot'la birlikte kullanıldığında da sohbeti Tor ağı üzerinden yönlendirebilir.
- **Google Play**: Android uygulamalarının bulunabileceği ve indirilebileceği depo.
- **GNU/Linux** - Microsoft Windows'a alternatif sağlayan bir FOSS işletim sistemi.
- **Güvenlik duvarı** - Bilgisayarınızı güvenilmez bağlantılardan ya da yerel ağlardan ve internetten koruyan bir araç
- **Güvenlik kablosu** - Bir dizüstü bilgisayar ya da harici sürücüler ve bazı masaüstü bilgisayarlar dahil diğer donanım parçalarını fiziksel olarak alınıp götürülmesini engellemek için bir duvara ya da masaya sabitlemekte kullanılabilecek kilitli bir kablo
- **Güvenlik politikası** - Kuruluşunuzun çeşitli tehditlere karşı en iyi nasıl korunacağını betimleyen ve güvenlikle ilgili belirli olaylar olduğunda atılması gereken adımların listesini içeren yazılı bir belge.
- **Guardian Project**: Güvenlik ve gizlilik öncelikli akıllı telefon uygulamaları, mobil cihazlar için işletim sistemi zenginleştirmeleri ve özelleştirmeleri oluşturan bir örgüt.
- **Güvenlik sertifikası** - Güvenli web sitelerinin ve diğer internet servislerinin şifreleme kullanarak, olduklarını iddia ettikleri kişi olduklarını kanıtlamasının bir yolu. Tarayıcınızın bir *güvenlik sertifikasını* geçerli olarak kabul etmesi için hizmetin güvenilir bir örgütten bir *dijital imza* için ödeme yapması gerekir. Maliyetinin yüksek olmasından dolayı bazı hizmet operatörleri bu harcamayı yapamayacak durumda veya yapmaya isteksiz olabilir. Bu nedenle zaman zaman geçerli bir hizmeti ziyaret ederken bile bir güvenlik sertifikası hatası görebilirsiniz.
- **Güvenli Soket Katmanı/Secure Sockets Layer (SSL)** - Bilgisayarınızla ziyaret ettiğiniz bazı web siteleri ve internet servisleri arasında güvenli, *şifrelenmiş* bağlantıyı sürdürmenize izin veren teknoloji. SSL aracılığıyla bir web sitesine bağlandığınızda web sitesinin adresi *HTTP* yerine *HTTPS* ile başlayacaktır.
- **Güvenli şifre veri tabanı** - Tek bir master şifre kullanarak parolalarınızı şifreleyen ve depolayan bir araç

- **Hacker** - Bu kitapta sözü edilen bağlamda, hassas bilgilerinize erişmeye ya da bilgisayarınızın uzaktan denetimini ele geçirmeye çalışan, kötü niyetli bir bilgisayar suçlusu.
- **iPhone**: Apple'ın iOS işletim sistemiyle çalışan Apple tarafından tasarlanmış akıllı telefon markası.
- **İnternet Protokol Adresi (İp adresi)** - Bilgisayarınıza, internete bağlandığında atanan özgün kimlik.
- **İnternet Servis Sağlayıcısı (ISS)/Internet Service Provider (ISP)** - İnternete ilk bağlantınızı sağlayan şirket ya da kuruluş. Birçok ülkede hükümetler, bu ülkede faaliyet gösteren ISP'ler aracılığıyla, filtreleme ve izleme gibi araçları kullanarak, internet üzerinde denetim dayatır.
- **Infrared Data Association (IrDA)** - Kızılötesi ışık spektrumunu kullanarak kısa mesafe veri alışverişi için kablosuz bir fiziksel iletişim standardı. Modern cihazlarda IrDA'nın yerini Bluetooth almıştır.
- **IP Üzerinden Ses (VoIP)** - İnterneti diğer VoIP kullanıcıları ve telefonlarla sesli iletişim için kullanmanıza izin veren teknoloji.
- **Java Uygulamaları (Applets)** - Birçok işletim sistemi altında çalışabilen küçük programlardır. Bunlar sık sık web sayfaları içinde gelişmiş işlevler sağlamak için kullanılır.
- **Jailbreaking**: İşletim sistemine tam erişim elde etmek için iPhone'un üreticisi ya da mobil telekomünikasyon taşıyıcısı tarafından engellenmiş özelliklerini açma işlemi.
- **K9 Mail**: APG uygulamasıyla birlikte kullanıldığında OpenPGP şifrelemesini olanaklı kılan Android akıllı telefonlar için bir FOSS e-posta istemcisi.
- **Kalıcı silme işlemi** - Bilgileri güvenli ve kalıcı olarak silme süreci
- **Kara liste** - Sınırlayıcı filtreleme politikası nedeniyle erişilemeyen engellenmiş web sitelerinin ve diğer internet servislerinin bir listesi
- **Kaynak kodu** - Bilgisayar programcıları tarafından yazılan, yazılımların oluşturulmasına izin veren kod. Verili bir araç için kaynak kodu onun nasıl çalıştığını ya da güvenilmez ya da zararlı olup olmadığını açığa çıkarır.
- **KeePass** - Ücretsiz ve güvenli bir şifre veritabanı
- **Kesintisiz Güç Kaynağı (UPS)** - Önemli bilgisayar donanımınızın, ani güç kayıpları sırasında işlemesine ya da zarıfçe kapatılmasına izin veren bir ekipman.
- **Keylogger** - Bilgisayar klavyenizle hangi tuşlara bastığınızı kaydeden ve bunu başkalarına gönderen bir casus yazılım türü. Keylogger'lar çoğu zaman e-posta ve diğer parolaları çalmak için kullanılır.
- **Kötü Amaçlı Yazılımlar** - *Virüs, casus yazılım, truva atı* ve bu tür diğer tehditleri kapsayan kötü amaçlı yazılımlar için kullanılan genel bir terim
- **Küresel Konumlama Sistemi (GPS)** - Uzay-tabanlı küresel navigasyon uydu sistemi. Bu sistem tüm hava koşullarında, Dünya'ya yakın veya Dünya'nın üzerindeki herhangi bir yerde konum ve zaman bilgisi sağlar. (Tamamen) engellenmemiş gök görüntüsü olan her yerde çalışır.
- **LiveCD (Canlı CD)** - Bilgisayarınızın geçici olarak farklı bir işletim sistemi çalıştırmasını sağlayan bir CD.
- **Mnemonic device** - Karmaşık şifrelerinizi hatırlamanıza yardımcı olacak basit bir püf noktası
- **NoScript** - Tanımadığınız web sayfalarında bulunabilecek kötü amaçlı programlara karşı bilgisayarınızı koruyan Firefox tarayıcısı için güvenlik eklentisi
- **Obscuracam**: Fotoğraflardaki kişilerin yüzlerini bulanıklaştırmak gibi değişiklikleri kolaylaştırarak insanların kimliklerini koruyan, Android akıllı telefonlar için bir FOSS uygulaması.
- **Orbot**: Orweb ve Gibberbot gibi uygulamaların Tor ağına bağlanmasını sağlayan, Android akıllı telefonlar için bir FOSS uygulaması.
- **Orweb**: Orbot'la birlikte kullanıldığında Tor ağı üzerinden tarama yapmayı kolaylaştıran, Android akıllı telefonlar için bir FOSS web tarayıcısı
- **Off the Record (OTR)** - Pidgin anlık mesajlaşma programı için bir şifreleme eklentisi
- **Sahipli Yazılımlar** - Ücretsiz ve Açık Kaynak Kodlu Yazılımın (FOSS) karşıtı. Bu uygulamalar genellikle ticaridir ama sınırlayıcı yasal zorunlulukları olan *ücretsiz yazılım* da olabilirler.
- **Peacefire** - Bu ücretsiz hizmetin aboneleri, internet sansürünü aşmak için kullanılacak proxy'lerin güncellenmiş bir listesini içeren e-postaları düzenli aralıklarla alır.
- **Pidgin** - *Off the Record (OTR)* olarak adlandırılan şifreleme eklentisini destekleyen bir FOSS anlık mesajlaşma aracı

- **Proxy** - İnternet iletişiminizin bir kısmını ya da tamamını aracılığıyla yönlendirebileceğiniz ve internet sansürünü aşmakta kullanabileceğiniz bir aracılık hizmeti. Bir proxy kamuya açık olabilir ya da ona erişmek için bir kullanıcı adı ve şifreyle giriş yapmanız gerekebilir. Proxy'lerin sadece bazıları güvenlidir; bu da bilgisayarınız ve proxy aracılığıyla bağlandığınız internet servisleri arasında gidip gelen bilginin gizliliğini korumak için şifreleme kullandıkları anlamına gelir.
- **RiseUp** - Aktivistler tarafından aktivistler için işletilen, webmail aracılığıyla ya da *Mozilla Thunderbird* gibi bir e-posta istemcisi kullanarak güvenli bir biçimde erişilebilen bir e-posta hizmeti.
- **Rooting**: Android telefonun, işletim sistemine tam erişim elde etmek için üreticileri tarafından engellenmiş özelliklerini açma işlemi.
- **Sansür aşma** - Engellenmiş web sitelerine ve diğer internet servislerine erişmek için internet filtrelerini aşma eylemi
- **SİM kartı** - Belirli bir telefon şirketinin hizmetini alabilmek için cep telefonlarına takılabilen küçük çıkarılabilir bir kart. SİM kartlara telefon numaraları ve yazılı mesajlar kaydedilebilir.
- **Skype** - Diğer Skype kullanıcılarıyla ücretsiz konuşmanızı ve telefonları ücretsiz aramanızı sağlayan ücretsiz bir IP Üzerinden Ses (VoIP) aracı. Skype'ı üreten firma diğer Skype kullanıcılarıyla konuşmaların şifrelendiğini iddia etmektedir. Kapalı-kaynaklı bir araç olduğundan bu iddiayı doğrulamanın hiçbir yolu yoktur ama birçok kişi bunun doğru olduğuna inanmaktadır. Skype ayrıca anlık mesajlaşmayı da desteklemektedir.
- **Spybot** - Casus yazılımlara karşı bilgisayarınızı tarayan, casus yazılımları silen ve bilgisayarınızı korumaya yardım eden ücretsiz ve kötü amaçlı yazılımlara karşı bir araç
- **Steganografi (Steganography)** - Hassas bilgilerin, dikkat çekmekten kaçınmak için başka bir şeymiş gibi görünmesini sağlamak ve gizlemek için kullanılan yöntem
- **Sunucu** - Bir web sayfasını barındırmak ya da diğer bilgisayarlara e-posta göndermek ve onlardan e-posta almak için internete bağlanan ve açık bırakılan bir bilgisayar
- **Swap file** - Bilgisayarın performansını arttırmak amacıyla, bazıları hassas olabilecek bilgilerin zaman zaman kaydedildiği bir dosya
- **Şifreleme** - Bilgiyi matematik kullanarak *şifrelemenin* veya *kariştirmanın* bir yolu. Şifrelenmiş bir bilginin şifresi, sadece şifre ya da *şifreleme anahtarı* gibi spesifik bir bilgiye sahip olan birisi tarafından çözülebilir.
- **Temel Giriş/Çıkış Sistemi (BIOS)** - Bir bilgisayardaki yazılımın ilk ve en derin kademesi. BIOS, başlangıç şifresi dahil bilgisayarın donanımıyla ilgili ileri düzey tercihlerinizi ayarlamaya izin verir.
- **Textsecure**: Şifrelenmiş metin tabanlı mesajları göndermeyi ve depolamayı kolaylaştıran Android için bir FOSS uygulaması.
- **Thunderbird** - Enigmail şifreleme eklentisini desteklemek dahil bir dizi güvenlik özelliğine sahip FOSS e-posta programı.
- **Tor** - İnternet sansürünü aşmanın ve ziyaret ettiğiniz web sitelerini ve internet servislerini internet bağlantınızı izleyen herhangi birinden gizlemenin yanında bu web sitelerinde konumunuzu gizlemenize de izin veren bir anonimlik aracı.
- **TrueCrypt** - Hassas bilgilerinizi güvenli olarak depolamanıza izin veren, FOSS dosya şifreleme aracı
- **Undelete Plus** - Yanlışlıkla silmiş olduğunuz bilgileri bazen kurtarabilen ücretsiz yazılım bir araç
- **Ücretsiz ve Açık-Kaynak Kodlu Yazılım (FOSS)** - Yazılımların bu türü ücretsiz olarak edinilebilir ve bir kullanıcının yazılımı sınamasını, paylaşmasını ve dönüştürmesini engelleyen yasal bir sınırlama yoktur.
- **Ücretsiz Yazılım** - Yazılımın oluşturulmasında kullanılan kaynak koda kullanıcının erişimini engelleyen hukukî ya da teknik sınırlamalara tabi; fakat ücretsiz olan yazılımlar
- **VaultletSuite 2 Go** - Ücretsiz bir şifrelenmiş e-posta programı
- **Windows Phone**: Microsoft tarafından geliştirilmiş bir akıllı telefon işletim sistemi.
- **Your-Freedom** - Özel bir proxy aracılığıyla internete bağlanarak engellemeleri aşmanızı sağlayan ücretsiz bir sansür aşma aracı. Your-Freedom uygun bir şekilde düzenlenirse proxy'lere olan bağlantılarınız iletişiminizin gizliliğini korumak için şifrelenecektir.
- **Yönlendirici (Router)** - Aracılığıyla bilgisayarların yerel ağlara bağlandığı ya da çeşitli yerel ağların internete eriştiği bir ağ donanımı. Uygun donanımlı bilgisayarlar için kablolu *erişim noktaları anahtarlar (switches)*, *ağ geçitleri* ve *hub'lar* yönlendiricinininkine benzer görevleri yerine getirir. Kablolu erişim noktaları da bu işlevleri yerleşik kablolu ağ ekipman donanımına sahip bilgisayarlar için yerine getirir.

Bağlantılar:

- [1] <https://info.securityinabox.org/tr/glossary#Hacker>
- [2] <https://info.securityinabox.org/tr/glossary#Malware>
- [3] <https://info.securityinabox.org/tr/glossary#Avast>
- [4] <https://info.securityinabox.org/tr/glossary#Spybot>
- [5] https://info.securityinabox.org/tr/glossary#Comodo_Firewall
- [6] https://info.securityinabox.org/tr/glossary#GNU_Linux
- [7] <https://info.securityinabox.org/tr/glossary#FOSS>
- [8] <https://info.securityinabox.org/tr/glossary#Freeware>
- [9] https://info.securityinabox.org/en/avast_main
- [10] https://info.securityinabox.org/tr/glossary#Clam_Win
- [11] https://info.securityinabox.org/en/howtouseavast#Section_3.2.1
- [12] https://info.securityinabox.org/en/spybot_main
- [13] <https://info.securityinabox.org/tr/glossary#Firefox>
- [14] https://info.securityinabox.org/en/firefox_main
- [15] https://info.securityinabox.org/en/firefox_noscript
- [16] <https://info.securityinabox.org/tr/glossary#NoScript>
- [17] https://info.securityinabox.org/en/comodofirewall_main
- [18] https://info.securityinabox.org/tr/chapter_1_5
- [19] <https://info.securityinabox.org/tr/glossary#Router>
- [20] https://info.securityinabox.org/tr/glossary#Proprietary_software
- [21] https://info.securityinabox.org/tr/glossary#Source_code
- [22] <https://www.libreoffice.org/>
- [23] <http://www.ubuntu.com/>
- [24] <https://info.securityinabox.org/tr/glossary#LiveCD>
- [25] <http://www.frontlinedefenders.org/esecman>
- [26] <http://www.virusbtr.com>
- [27] <http://www.marksanborn.net/howto/turn-off-unnecessary-windows-services>
- [28] <http://tacticaltech.org>
- [29] <http://www.askvg.com/download-free-bootable-rescue-cds-from-kaspersky-bitdefender-avira-f-secure-and-others/>
- [30] <http://www.selectrealsecurity.com/malware-removal-guide>
- [31] https://info.securityinabox.org/tr/glossary#Security_policy
- [32] https://info.securityinabox.org/tr/glossary#Physical_threats
- [33] https://info.securityinabox.org/tr/glossary#Physical_threat
- [34] <https://info.securityinabox.org/tr/glossary#Skype>
- [35] <https://info.securityinabox.org/tr/glossary#Server>
- [36] https://info.securityinabox.org/tr/glossary#Security_cable
- [37] <https://info.securityinabox.org/tr/chapter-3>
- [38] <https://info.securityinabox.org/tr/glossary#BIOS>
- [39] <https://info.securityinabox.org/tr/glossary#Bootling>
- [40] <https://info.securityinabox.org/tr/glossary#Encryption>
- [41] <https://info.securityinabox.org/tr/chapter-4>
- [42] <https://info.securityinabox.org/tr/glossary#UPS>
- [43] <https://info.securityinabox.org/tr/chapter-5>
- [44] https://info.securityinabox.org/tr/chapter_2_5
- [45] <http://www.frontlinedefenders.org/manuals/protection>
- [46] <http://www.frontlinedefenders.org/security-training>
- [47] <https://info.securityinabox.org/tr/glossary#KeePass>
- [48] https://info.securityinabox.org/tr/glossary#Secure_password_database
- [49] https://info.securityinabox.org/tr/chapter_3_2
- [50] https://info.securityinabox.org/tr/glossary#Mnemonic_device
- [51] https://passfault.appspot.com/password_strength.html
- [52] https://info.securityinabox.org/en/keepass_main
- [53] <http://en.wikipedia.org/wiki/Password>
- [54] http://en.wikipedia.org/wiki/Password_strength
- [55] http://en.wikipedia.org/wiki/Password_cracking
- [56] <https://info.securityinabox.org/tr/chapter-1>
- [57] <https://info.securityinabox.org/tr/chapter-2>
- [58] <https://info.securityinabox.org/tr/glossary#TrueCrypt>
- [59] https://info.securityinabox.org/en/truecrypt_main
- [60] https://info.securityinabox.org/tr/chapter_4_2
- [61] <https://info.securityinabox.org/tr/chapter-6>
- [62] <https://info.securityinabox.org/tr/glossary#Steganography>
- [63] https://info.securityinabox.org/tr/chapter_4_3
- [64] <http://www.truecrypt.org/docs/>
- [65] <http://www.truecrypt.org/faq.php>
- [66] https://info.securityinabox.org/tr/glossary#Cobian_Backup
- [67] <https://info.securityinabox.org/tr/glossary#Recuva>
- [68] <https://info.securityinabox.org/tr/glossary#Firewall>
- [69] <https://info.securityinabox.org/tr/glossary#Thunderbird>
- [70] https://info.securityinabox.org/en/thunderbird_main
- [71] https://info.securityinabox.org/tr/glossary#CD_burner
- [72] https://info.securityinabox.org/tr/chapter_5_5
- [73] https://info.securityinabox.org/en/cobian_main
- [74] https://info.securityinabox.org/en/recuva_main
- [75] <https://www.wuala.com/>
- [76] <https://spideroak.com/>
- [77] <https://drive.google.com/start>
- [78] <https://tahoe-lafs.org/trac/tahoe-lafs>
- [79] http://en.wikipedia.org/wiki/Data_recovery
- [80] <https://info.securityinabox.org/tr/glossary#Eraser>
- [81] <https://info.securityinabox.org/tr/glossary#Wiping>
- [82] <https://info.securityinabox.org/tr/glossary#CCleaner>
- [83] https://info.securityinabox.org/tr/glossary#Swap_file
- [84] https://info.securityinabox.org/en/eraser_main
- [85] <https://info.securityinabox.org/tr/glossary#Cookie>
- [86] https://info.securityinabox.org/en/ccleaner_main

[87] <http://www.piriform.com/ccleaner/faq>
[88] http://www.userix.org/publications/library/proceedings/sec96/full_papers/gutmann/
[89] http://en.wikipedia.org/wiki/Gutmann_method
[90] <https://jitsi.org/>
[91] <https://info.securityinabox.org/tr/glossary#VoIP>
[92] <https://info.securityinabox.org/tr/glossary#RiseUp>
[93] <https://info.securityinabox.org/tr/glossary#Pidgin>
[94] <https://info.securityinabox.org/tr/glossary#OTR>
[95] <https://info.securityinabox.org/tr/glossary#Enigmail>
[96] <https://info.securityinabox.org/tr/glossary#Keylogger>
[97] https://info.securityinabox.org/tr/chapter_7_1#Keeping_your_webmail_private
[98] https://info.securityinabox.org/tr/chapter_7_1#Switching_to_a_more_secure_email_account
[99] https://info.securityinabox.org/tr/chapter_7_4
[100] https://info.securityinabox.org/tr/chapter_7_4#Encrypting_and_authenticating_individual_email_messages
[101] https://info.securityinabox.org/tr/chapter_7_2
[102] <https://info.securityinabox.org/tr/glossary#ISP>
[103] <https://info.securityinabox.org/tr/glossary#SSL>
[104] <https://info.securityinabox.org/tr/discussion#Encryption>
[105] https://info.securityinabox.org/tr/glossary#Security_certificate
[106] https://info.securityinabox.org/tr/glossary#P_address
[107] https://info.securityinabox.org/tr/chapter_7_5
[108] <https://mail.riseup.net>
[109] https://info.securityinabox.org/en/riseup_main
[110] <https://info.securityinabox.org/tr/chapter-8>
[111] <https://info.securityinabox.org/tr/glossary#Tor>
[112] <https://info.securityinabox.org/tr/glossary#Circumvention>
[113] <https://info.securityinabox.org/tr/chapter-11>
[114] <https://info.securityinabox.org/en/dealingwithviruses#4.1>
[115] <https://info.securityinabox.org/en/dealingwithviruses#4.9>
[116] <http://www.libreoffice.org/>
[117] https://info.securityinabox.org/en/gpg4usb_portable
[118] https://info.securityinabox.org/en/pidgin_main
[119] <http://www.skype.com>
[120] <http://jitsi.org/>
[121] <http://www.google.com/talk>
[122] <http://voice.yahoo.com/>
[123] <http://explore.live.com/windows-live-messenger>
[124] https://info.securityinabox.org/tr/chapter_1_4
[125] <https://info.securityinabox.org/tr/glossary#VaultletSuite>
[126] https://info.securityinabox.org/en/vaultletsuite_main
[127] https://info.securityinabox.org/tr/glossary#Digital_signature
[128] https://info.securityinabox.org/en/thunderbird_encryption
[129] <https://help.riseup.net/en/email-clients>
[130] <https://mail.google.com/support/bin/topic.py?topic=12769>
[131] http://email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm
[132] https://secure.wikimedia.org/wikipedia/tr/wiki/Man-in-the-middle_attack
[133] <https://www.google.com/intl/tr/privacy/privacy-policy.html>
[134] http://news.cnet.com/8301-13578_3-9962106-38.html
[135] https://info.securityinabox.org/tr/glossary#Domain_name
[136] <https://info.securityinabox.org/tr/glossary#Proxy>
[137] <http://opennet.net/>
[138] <http://www.rsf.org/>
[139] <https://info.securityinabox.org/tr/glossary#Blacklist>
[140] https://info.securityinabox.org/tr/glossary#IP_addresses
[141] https://info.securityinabox.org/tr/glossary#Domain_names
[142] https://info.securityinabox.org/en/tor_main
[143] <https://info.securityinabox.org/tr/glossary%23Proxy>
[144] <https://info.securityinabox.org/tr/glossary#HTTPS>
[145] <https://info.securityinabox.org/tr/glossary#Psiphon>
[146] <https://info.securityinabox.org/tr/glossary#Peacefire>
[147] <https://info.securityinabox.org/tr/glossary#Encrypted>
[148] https://info.securityinabox.org/tr/chapter_8_5
[149] <https://help.riseup.net/en/riseup-vpn>
[150] <https://we.riseup.net/riseuphelp+en/vpn-howto>
[151] <http://www.hotspotshield.com/>
[152] <http://www.your-freedom.net/index.php?id=3>
[153] <http://www.your-freedom.net/index.php?id=170&L=0>
[154] <http://your-freedom.net>
[155] <https://www.your-freedom.net/index.php?id=172>
[156] <https://www.your-freedom.net/index.php?id=doc>
[157] <http://www.dit-inc.us/freerate>
[158] <http://www.addictivetips.com/windows-tips/freerate-lets-you-access-blocked-websites-at-optimal-speed/>
[159] <http://www.securitykiss.com/resources/download/>
[160] <http://www.securitykiss.com>
[161] <http://psiphon3.com>
[162] <http://peacefire.org/>
[163] <https://www.howtobypassinternetcensorship.org/>
[164] http://en.cship.org/wiki/Main_Page
[165] <http://citizenlab.org/guides/everyones-guide-english.pdf>
[166] http://www.rsf.org/IMG/pdf/Bloggers_Handbook2.pdf
[167] <http://advocacy.globalvoicesonline.org/tools/guide/>
[168] <https://www.eff.org/wp/locational-privacy>
[169] https://info.securityinabox.org/en/social_networking_tools
[170] <https://info.securityinabox.org/tr/glossary#GPS>
[171] https://info.securityinabox.org/tr/glossary#SIM_card
[172] <https://info.securityinabox.org/tr/node/3199>
[173] <https://info.securityinabox.org/tr/node/3200>

[174] <https://info.securityinabox.org/tr/node/3201>
[175] <https://info.securityinabox.org/tr/node/3202>
[176] <https://info.securityinabox.org/tr/glossary#Java>
[177] <https://info.securityinabox.org/tr/glossary#IrDA>
[178] <https://info.securityinabox.org/tr/glossary#Bluetooth>
[179] <http://mobiles.tacticaltech.org>
[180] <http://mobiles.tacticaltech.org/security>
[181] <http://www.activistsecurity.org/>
[182] http://www.freebeagles.org/articles/mobile_phones.html
[183] <http://mobileactive.org/mobilesecurity-citizenjournalism>
[184] http://sw.nokia.com/id/5274b81c-12d0-43bb-8d89-26f6a1ae111f/A_Brief_Introduction_to_Secure_SMS_Messaging_in_MIDP_en.pdf
[185] <http://www.mysecured.com/?p=127>
[186] <https://info.securityinabox.org/tr/chapter-10>
[187] <https://info.securityinabox.org/tr/Glossary#GPS>
[188] <https://info.securityinabox.org/tr/Glossary#FOSS>
[189] https://info.securityinabox.org/en/android_basic
[190] <http://f-droid.org>
[191] <https://info.securityinabox.org/tr/glossary#apk>
[192] https://info.securityinabox.org/tr/chapter_10_2_4
[193] https://info.securityinabox.org/tr/chapter_10_2_2
[194] <https://info.securityinabox.org/tr/Glossary#VoIP>
[195] <https://info.securityinabox.org/tr/glossary#skype>
[196] <https://info.securityinabox.org/tr/chapter-7>
[197] https://info.securityinabox.org/tr/chapter_7_3
[198] <http://f-droid.org/repository/browse/?fdid=com.csipsimple&fdpage=4>
[199] <https://guardianproject.info/wiki/OSTN>
[200] <https://ostel.me>
[201] <https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone>
[202] https://info.securityinabox.org/tr/chapter_10_2_3
[203] <https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms>
[204] https://info.securityinabox.org/en/textsecure_main
[205] <https://guardianproject.info/apps/gibber/>
[206] https://info.securityinabox.org/en/gibberbot_main
[207] <https://chatsecure.org>
[208] https://info.securityinabox.org/en/APG_main
[209] <https://code.google.com/p/cryptonite/>
[210] https://info.securityinabox.org/tr/chapter_11_7
[211] https://info.securityinabox.org/en/Cryptonite_main
[212] https://info.securityinabox.org/en/KeepassDroid_main
[213] https://info.securityinabox.org/tr/chapter_7_1
[214] https://info.securityinabox.org/en/K9_APG_main
[215] <https://guardianproject.info>
[216] <https://guardianproject.info/apps/obscuracam/>
[217] https://info.securityinabox.org/en/Obскурacam_main
[218] <https://info.securityinabox.org/tr/www.witness.org>
[219] <https://www.torproject.org/docs/android.html.en>
[220] https://info.securityinabox.org/en/Orbot_main
[221] https://info.securityinabox.org/en/Orweb_main
[222] <http://f-droid.org/repository/browse/?fdid=org.mozilla.firefox>
[223] <https://guardianproject.info/>
[224] <https://guardianproject.info/apps/proxymob-firefox-add-on/>
[225] <http://www.cyanogenmod.com>
[226] <http://www.cyanogenmod.com/devices>
[227] <https://play.google.com/store/apps/details?id=com.nemesis2.luksmanager&hl=en>
[228] <http://www.whispersys.com/whispercore.html>
[229] <https://help.riseup.net/en/vpn>
[230] <https://support.apple.com/kb/HT1424>